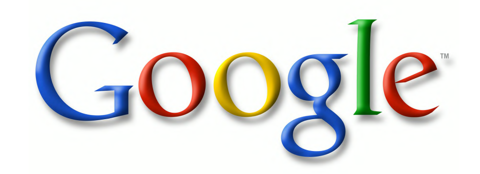












Elemente

der

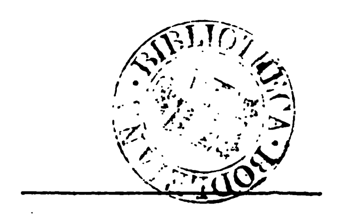
Zahlen-Theorie,

allgemein fasslich dargestellt

von

Dr. Herm. Schwarz,

Lehrer der Mathematik am Königl. Pädagogium zu Halle.



Halle,

Druck und Verlag von H. W. Schmidt.

1855.

Vorrede.

Die Entstehung dieses Werkes hängt mit einem mir ertheilten Auftrage zusammen, aus den Papieren des verstorbenen Prof. Sohncke dasjenige herauszusuchen, was sich zur eventuellen Herausgabe eigne. Ich fand nun unter dem Titel „Zahlentheorie“ eine Reihe von Abhandlungen, die die Kreistheilung zu ihrem Objecte haben und allerdings dazwischen eingestreut auch noch das Unentbehrlichste aus der reinen Arithmetik enthalten. Bei einer genaueren Durchsicht gewann ich indessen bald die Ueberzeugung, dass der erwähnte Gegenstand zu speciell und das die allgemeine Theorie Betreffende zu unvollständig wäre, um dem Werke einen allgemeineren Leserkreis zu sichern, und so entschloss ich mich nur die Einleitung daraus zu nehmen und übrigens in vollkommen selbständiger Weise die Elemente der Zahlentheorie zu schreiben.

Das Bedürfniss eines solchen Werkes ist wohl ausser Zweifel; denn trotz des grossen Interesses, welches die Neuzeit seit Euler, Lagrange und Gauss der Zahlentheorie zugewandt hat, fehlt es noch sehr an einem Lehrbuche, welches dem Anfänger zum Selbststudium diene. Zur Begründung dieser Behauptung genügt es wohl einfach auf die Thatsache hinzuweisen, dass seit den unsterblichen „disquisitiones arithmeticae“ von Gauss meines Wissens nur ein das Nothwendigste kurz zusammenstellendes Lehrbuch im Jahre 1832 erschienen ist, nämlich „die Anfangsgründe der höheren Arithmetik“ von Minding*). Indem ich die Ausfüllung der aufgezeigten Lücke in der mathematischen Literatur übernommen habe, bin ich mir recht wohl der Schwierigkeiten meiner Aufgabe bewusst und nehme

*) Scheffler's unbestimmte Analytik ist mir erst nach Beendigung meines Manuscripts in die Hände gekommen.

das nachsichtige Urtheil Sachverständiger in Anspruch. Es sind namentlich zwei Hauptschwierigkeiten, die eine mehr formale von Seiten der Darstellung, die andere mehr materiale von Seiten des Inhaltes.

Formell habe ich eine zusammenhängende Darstellung angestrebt, welche einmal ohne der Strenge der Argumentation etwas zu vergeben, nicht mehr als das Mass der Kenntnisse eines Abiturienten von einem Gymnasium oder einer Realschule voraussetzt, und dann die einzelnen Lehrsätze und Aufgaben nicht als etwas für sich Abgesondertes behandelt, sondern soviel als möglich ihren Zusammenhang mit dem Gange der allgemeinen Entwickelung hervorhebt. Zugleich habe ich eine grosse Menge bis ins kleinste Detail durchgerechneter Beispiele mit eingestreut und an vielen Orten für ein ausreichendes Material zu selbstständigen Uebungen gesorgt.

Materiell handelte es sich vor allem um eine zweckmässige Auswahl aus der reichen Fülle des gebotenen Stoffes. Hier sind vornehmlich zwei Rücksichten für mich massgebend gewesen, zuerst der möglichst genaue Anschluss an die disquisitiones arithmeticae, weil diese als der Ausgangspunkt und das Fundament aller neueren zahlentheoretischen Entwickelungen angesehen werden müssen, und dann die Beschränkung auf die allgemeine Theorie der Potenzreste und der Gleichungen zweiten Grades. Diese Beschränkung schien mir um so nöthiger, da ich die Grenzen des Elementaren nicht überschreiten und doch etwas Fertiges und in sich Abgeschlossenes liefern wollte. Nur an einer Stelle der Einleitung findet sich eine Ausnahme. Es ist nämlich daselbst der bekannte Euler'sche Satz behandelt über die merkwürdige Abhängigkeit, welche zwischen der Theilersumme einer Zahl und der Reihe der Pentagonalzahlen besteht. Aber dieser Satz ist für das Verständniss des Nachfolgenden unwesentlich und kann von dem Anfänger, welcher des höheren Calcüls unkundig ist, ohne Schaden übergangen werden.

Halle, den 15. Juni 1855.

Der Verfasser.

Inhaltsverzeichniss.

Einleitung.

§. 1.

Die alten Griechen theilten die Mathematik in drei Theile, in Geometrie, Logistik und Arithmetik. Die Geometrie, welche sie zu einem hohen Grade von Ausbildung brachten, besteht nach ihren Grundzügen noch jetzt in unveränderter Gestalt fort; die Logistik begreift die Kunst des gewöhnlichen Rechnens in sich, in der es auf den λόγος, das Verhältniss der einen Grösse zur Einheit ankommt, gleichgültig, was die Grösse ist, ob eine ganze oder gebrochene Zahl; sie ist in neuerer Zeit ein specieller Theil der Algebra geworden. Die Arithmetik endlich ist die Wissenschaft von den ganzen Zahlen und erscheint, wie die Logistik, im griechischen Alterthume nur wenig ausgebildet, weil ihr zwei wesentliche Dinge abgingen, die allgemeine Bezeichnung der Zahlen und ein zweckmässiges Zahlensystem. Das Beste, welches uns aus jener Zeit überkommen ist, sind des Diophantus problemata arithmetica, in denen gewisse Aufgaben in ganzen und rationalen Zahlen aufgelöst werden. Das Werk steht einzig und räthselhaft da, denn von allen übrigen Werken kann man eine successive Entstehung angeben, wie z. B. bei denen des Euclides, der mehr nur das früher Gefundene zu einem Ganzen zusammenstellte. Aber von des Diophantus Theorie findet man weder vor, noch nach ihm eine Spur; er selbst ist gleicher Massen eine problematische Person und soll im 4ten Jahrhundert gelebt haben. Alle gleichzeitigen arithmetischen Werke stehen so weit unter ihm, dass sich gar keine Verbindung auffinden lässt. Man glaubte daher neuerlich, dass die Alexandriner zur Kenntniss dieser Wissenschaft durch Handelsverkehr mit den Indiern gelangt wären, denn von letzteren hat man Werke, wenn auch späteren Ursprunges, in denen diese Art von Problemen und noch manches Andere, wie z. B. die Theorie der Kettenbrüche, be-

handelt wird. Colebroocke hat diese Indischen Probleme ganz in der Art der Inder zusammengestellt, die alles in Form von Kunststücken vortrugen. Wahrscheinlich sind die gleichartigen Werke der Griechen verloren gegangen.

Euclid handelt im 7ten, 8ten, 9ten Buche von den Anfangsgründen der Arithmetik. Bei ihm findet man zuerst den Namen Primzahl (*ἀριϑμὸς πρῶτος*) erwähnt und den Satz, dass es unendlich viele Primzahlen gäbe. Der Beweis ist folgender. Wäre die Anzahl der Primzahlen begrenzt und n die äusserste Grenze, so müsste eine Zahl von der Form

$$1.\ 2.\ 3.\dots.\ (n-1)n+1$$

nothwendig entweder selbst eine Primzahl sein oder aber durch eine grössere Primzahl, als n ist, ohne Rest theilbar sein, weil alle Primzahlen von 1 bis n in jene Summe hineindividirt 1 zum Reste lassen. In beiden Fällen mithin existirt eine Primzahl grösser als n, im Widerspruche zu der Voraussetzung.

Ferner ist bereits Eratosthenes der Erfinder einer Methode gewesen, vermöge deren die Primzahlen aus der Reihe der übrigen Zahlen ausgeschieden werden. Man bildet sich nämlich die Reihe der ungeraden Zahl von 3 ab bis zu irgend einer Grenze und wirft, von 3 aus gerechnet, die 3te, 6te, 9te, ... Zahl weg, also die Zahlen 9, 15, 21, ..., weil sie offenbar durch 3 theilbar sind. Hierauf streicht man von 5 ab die 5te, 10te, 15te, ... Zahl, also 15, 25, 35, ... (hierbei werden die bereits wegen 3 gestrichenen Zahlen wieder mit gezählt); allgemein: man wirft von der nächsten stehen gebliebenen Primzahl n ab die $n$te, $2n$te, $3n$te .... Zahl als durch n theilbar weg und setzt das Verfahren so weit fort, bis man zu derjenigen Primzahl kommt, welche nächst kleiner ist als die Quadratwurzel aus der gegebenen Grenze. Denn es ist leicht einzusehen, dass, wenn man die nachfolgenden Primzahlen mit in Rechnung bringen wollte, bis zu der gegebenen Grenze hin nur solche Zahlen noch wegfallen, welche bereits gestrichen sind. Mithin sind die stehen bleibenden Zahlen innerhalb dieses Intervalles die Reihe der Primzahlen. Suchen wir z. B. alle Primzahlen bis 100, so ist die Primzahl, welche nächst kleiner ist zu $\sqrt{100}$, offenbar 7 und dem zu Folge hat man blos die Primzahlen 3, 5, 7 in Berücksichtigung zu ziehen, und das Sieb des Eratosthenes bekommt folgende Gestalt:

3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99.

Im 16ten Jahrhundert, zur Zeit des Descartes, nahm man die Zahlentheorie wieder auf und zwar war es die Kenntnissnahme von des Diophantus Schriften, welche den ersten Anstoss hierzu gab. Wir haben 2 Ausgaben der Diophantischen Probleme aus jener Zeit, eine von Bachetus de Meziriac und die andere, ungleich bedeutendere, von Fermat, Parlamentsrath zu Toulouse. In den Noten zu letzterer finden sich viele Sätze über Primzahlen und ganze Zahlen, von denen der Verfasser den Beweis theilweise nicht besass. Diese Sachen gingen nun auf die folgenden Mathematiker über und erschienen so schwer, dass man, um sie zu beweisen, die ganze Arithmetik schaffen musste. Diophantus sagt einmal, man zerfälle die Zahl in 4 Quadrate. Daher scheint der Satz vorauszugehen, dass jede Zahl aus 4 Quadraten zusammengesetzt werden könne. Weiter heisst es, die Zahl $4n+1$ ist immer die Summe zweier Quadrate. Fermat fügt hinzu, jede ganze Zahl ist gleich der Summe von 3 dreieckigen, 4 viereckigen u. s. w. Zahlen. Von diesen Sätzen hat Euler den einen: jede ganze Zahl sei gleich der Summe von 4 Quadraten, zu beweisen versucht, doch fand den allgemeinen Beweis erst Lagrange. Den Satz, dass jede Zahl gleich der Summe dreier dreieckigen Zahlen sei, bewies Gauss und den allgemeinen Beweis für alle Fälle fand Cauchy. Die Methoden, die Fermat zu den Beweisen anwandte, sind verloren gegangen, doch müssen sie sehr einfach gewesen sein. Von den Sätzen, die er noch nicht beweisen zu können eingesteht, haben sich mehrere als unrichtig gezeigt. So sagte er, die Zahl

$$2^{(2^n)}+1$$

sei immer eine Primzahl, aber Euler fand, dass $2^{32}+1$ durch 641 theilbar sei. Es finden sich auch bereits bei Fermat mehrere sogenannte negative Sätze, welche die Unmöglichkeit gewisser Zahlformen aussprechen; z. B.: die Summe zweier gleich hohen Potenzen kann niemals wieder eine Potenz desselben Grades geben, ausgenommen wenn der Exponent 2 ist. Euler bewies diesen Satz für die 3te und 4te Potenz, Legendre für die 5te und Dirichlet für die 14te Potenz. Wie ungefähr Fermat geschlossen haben

mag, zeigt die folgende Bemerkung: Er zeigt, dass, wenn eine Gleichung für gewisse ganze positive Zahlen stattfindet, sie auch stattfinden muss für kleinere ganze Zahlen. Da diese sich aber nicht bis ins Unendliche verkleinern lassen, so kann es keine solchen Zahlen geben. — Ausser Fermat beschäftigten sich gleichzeitig mit der Zahlentheorie Frenicle de Bessi, Wallis und Lord Brounker.

In der Folgezeit, welcher die grossen Entdeckungen im höheren Calcül angehören, blieb die Theorie der Zahlen liegen. Erst in der zweiten Hälfte des vorigen Jahrhunderts wurde der Gegenstand wieder in Anregung gebracht und zwar von Euler, Lagrange und Legendre. Von des letzteren Werk hat die Wissenschaft den Namen Zahlentheorie. Zu einem ordentlichen Abschlusse aber gelangten alle diese Arbeiten erst durch die Disquisitiones arithmeticae, welche Gauss im Jahre 1800 als 22jähriger Jüngling herausgab. Einzelne interessante Abhandlungen finden sich in der Neuzeit in Crelle's Journal zerstreut, namentlich solche von Dirichlet und Kummer.

§. 2.

Indem wir jetzt näher auf unseren Gegenstand eingehen, müssen wir unterscheiden zwischen Algebra und Arithmetik, welche letztere jetzt indessen gewöhnlicher Zahlentheorie oder auch unbestimmte Analysis heisst. Jene handelt von den Zahlen im Allgemeinen; diese bezieht sich nur auf die Eigenschaften rationaler, ja meistentheils ganzer Zahlen. Sie lehrt einerseits die Natur der Zahlen kennen, andererseits Zahlen finden, welche gewissen Bedingungen genügen. Der Name unbestimmte Analysis rührt davon her, weil derartige Aufgaben meistens mehrere oder gar unendlich viele Auflösungen gestatten.

Der Zahlentheorie gehören viele den Elementen einverleibte Sätze an, z. B.

Die Ordnung der Faktoren bei der Multiplikation ist gleichgültig.

und

Wenn zwei Zahlen beide durch eine Primzahl nicht theilbar sind, so ist auch ihr Produkt nicht durch jene Primzahl theilbar.

Wir wollen wenigstens den letzteren wichtigen Satz beweisen und ihm zu dem Zwecke gleich die etwas allgemeinere Form geben:

Wenn zwei Zahlen beide zu einer dritten relative Primzahlen sind, so ist auch noch ihr Produkt zu dieser dritten relative Primzahl.

Seien a und b zwei beliebige ganze Zahlen und p eine zu beiden relative Primzahl, die also weder mit a noch mit b einen gemeinschaftlichen Faktor ausser der Einheit hat: dann kann man nach einander

$$a = qp + a' \quad (a' < p),$$
$$p = q'a' + a'' \quad (a'' < a'),$$
$$p = q''a'' + a''' \quad (a''' < a''),$$
$$\cdots\cdots\cdots$$
$$\cdots\cdots\cdots$$
$$p = q^{(n-1)} a^{(n-1)} + a^{(n)} \left(a^{(n)} < a^{(n-1)}\right)$$

setzen, wenn man unter a', a'', a''', a^{IV}, ... $a^{(n)}$ die Reste versteht, welche bei der Division von a durch p und von p nach einander durch a', a'', a''', ... $a^{(n-1)}$ bleiben. Aus diesen Gleichungen erhellt, dass die a', a'', ... $a^{(n)}$ keinen gemeinschaftlichen Faktor mit p haben können; denn hätte zunächst a' mit p einen gemeinschaftlichen Faktor, so müsste er auch ein Faktor von a sein, also a mit p einen gemeinschaftlichen Faktor haben gegen die Voraussetzung. Aus demselben Grunde, da p und a' relative Primzahlen sind, müssen es wegen der zweiten Gleichung p und a'' sein, und wegen der folgenden Gleichung p mit a''' u. s. w. fort. Weiter erhellt unmittelbar, dass die verschiedenen a sich fortwährend verkleinern. Die Grenze dieser Verkleinerung kann aber nicht 0 sein; denn nähme man $a^{(n)} = 0$ und wäre $a^{(n-1)}$ hierbei von 1 verschieden, so wäre $a^{(n-1)}$ ein Faktor von p, während doch beide relative Primzahlen sein müssen. Dem zu Folge muss man mit Nothwendigkeit, wenn man die Rechnung hinreichend fortsetzt, schliesslich auf einen Endrest

$$a^{(n)} = 1$$

kommen. Dieses vorausgesetzt multiplizire man die vorstehenden Gleichungen sämmtlich mit b, so folgt

$$ab = qpb \quad + a'b,$$
$$pb = q'a'b \quad + a''b,$$
$$pb = q''a''b + a'''b,$$
$$\cdots\cdots$$
$$\cdots\cdots$$
$$\cdots\cdots$$
$$pb = q^{(n-1)}a^{(n-1)}b + a^{(n)}b.$$

Wäre nun ab durch p theilbar, so könnte die rechte Seite der ersten Gleichung nicht anders durch p aufgehen, als indem auch $a'b$ durch p aufginge. Weil nun $a'b$ durch p aufginge, müsste dasselbe wegen der zweiten Gleichung auch $a''b$ und indem man so weiter schliesst, erhielte man zuletzt, dass

$$a^{(n)}b = 1 \,.\, b = b$$

durch p ohne Rest dividirbar wäre, was im Widerspruche gegen die Voraussetzung stände, nach der b und p relative Primzahlen sind. Damit fällt denn auch die erste Annahme, dass ab die Zahl p zum Theiler haben könne, eben so wenig kann ab einen Factor von p zum Theiler haben.

Wir wollen an dieser Stelle noch ein allgemeines Theorem aufführen, welches aus Crelle's Zahlentheorie entnommen ist und den in den Elementen aufgenommenen Sätzen über die Theilbarkeit der Zahlen zu Grunde liegt.

Bekanntlich kann jede beliebige ganze Zahl Z durch einen Ausdruck von der Form:

$$Z = x_m A^m + x_{m-1} A^{m-1} + n_{m-2} A^{m-2} + x_{m-3} A^{m-3} + \ldots$$
$$+ x_2 A^2 + x_1 A + x_0$$

dargestellt werden, wo A eine beliebige ganze Zahl und x_m, x_{m-1}, ... x_0 bestimmte ganze Zahlen, die kleiner als A sind, bedeuten; und dieser Ausdruck geht geradezu in den gewöhnlichen dekadischen Ausdruck von Z über, wenn man $A = 10$ nimmt. Dieses vorausgesetzt setze man

$$nA = qs + r,$$

wo s irgend eine willkürliche ganze Zahl bezeichnet und n gleichfalls, nur mit der Beschränkung, dass es eine relative Primzahl zu s ist, r dagegen den Rest vorstellt, der bei der Division von nA durch s bleibt. Alsdann geht Z durch die Zahl s auf oder geht nicht auf, je nachdem der Zahlenausdruck

$$z = x_m r^m + x_{m-1} n r^{m-1} + x_{m-2} n^2 r^{m-2} + \ldots\ldots$$
$$+ x_2 n^{m-2} r^2 + x_1 n^{m-1} r + x_0 n^m$$

durch s aufgeht oder nicht aufgeht.

Um dieses Theorem zu erweisen erhebe man die Gleichung für nA nach einander auf die zweite, dritte, ... Potenz; es folgt

$$n^2A^2 = (q^2 s + 2qr)s + r^2,$$
$$n^3A^3 = (q^3s^2 + 3q^2sr + 3qr^2)s + r^3,$$
$$\ldots\ldots\ldots$$
$$\ldots\ldots\ldots$$

und indem man die ganzzahligen Ausdrücke in den Parenthesen mit q_1, q_2, ... bezeichnet, kann man das Gleichungssystem aufstellen:

$$nA = qs + r,$$
$$n^2A^2 = q_1 s + r^2,$$
$$n^3A^3 = q_2 s + r^3,$$
$$\ldots\ldots$$
$$\ldots\ldots$$
$$n^m A^m = q_{m-1} s + r^m.$$

Diese Ausdrücke setze man in die Gleichung für Z ein, nachdem man dieselbe zuvor mit n^m multiplizirt und dem Produkte die Form

$$n^m Z = x_m n^m A^m + x_{m-1} n n^{m-1} A^{m-1} + x_{m-2} n^2 n^{m-2} A^{m-2} + \ldots\ldots$$
$$+ x_2 n^{m-2} n^2 A^2 + x_1 n^{m-1} nA + x_0 n^m$$

gegeben hat. Dadurch erhält man

$$n^m Z = x_m \left(q_{m-1} s + r^m \right)$$
$$+ x_{m-1} n \left(q_{m-1} s + r^{m-1} \right)$$
$$+ x_{m-1} n^2 \left(q_{m-3} s + r^{m-2} \right)$$
$$\ldots\ldots\ldots$$
$$\ldots\ldots\ldots$$
$$+ x_2 n^{m-2} (q_1 s + r^2)$$
$$+ x_1 n^{m-1} (qs + r)$$
$$+ x_0 n^m$$

Zieht man hier alle die Glieder, welche in s multiplizirt sind, zu einem einzigen zusammen, so erhält man einen ganzzahligen Coefficienten der Grösse s, den wir augenblicklich mit Q bezeichnen wollen, und können, da die auf der rechten Seite noch ausserdem übrig bleibenden Glieder geradezu unseren obigen Ausdruck z geben, ganz einfach schreiben:

$$n^m Z = Qs + z.$$

Hieraus erhellt aber, dass, wenn s in z aufgeht, es auch in $n^m Z$ aufgehen muss, und dies ist, da n eine relative Primzahl zu s ist, nicht anders möglich, als wenn s ein Theiler von Z ist. Weiter erhellt, dass, sofern man $n = 1$ hat, die Zahlen Z und z durch s dividirt denselben Rest lassen.

1) Theilbarkeit der Zahlen durch 3 und 9. Setzt man s nacheinander gleich 3 und 9, so wird die Gleichung

$$nA = qs + r$$

beide Male durch die Werthe

$$A = 10, \; n = 1, \; r = 1$$

befriedigt und es folgt

$$z = x_0 + x_1 + x_2 + \dots + x_{m-1} + x_m;$$

mithin, da die x, weil $A = 10$ ist, geradezu die auf einander folgenden Ziffern der dekadischen Zahl Z bedeuten, erhalten wir den bekannten Satz: Eine Zahl lässt durch 3 oder 9 dividirt denselben Rest, den ihre Quersumme durch dieselben Zahlen dividirt lässt; sie ist demgemäss durch 3 oder 9 theilbar, wenn es ihre Quersumme ist.

2) Theilbarkeit der Zahlen durch 7, 11, 13. Setzen wir

$$A = 1000, \; r = -1, \; n = +1,$$

so wird unsrer Gleichung

$$nA = qs + r$$

gleichmässig Genüge geleistet durch die 3 Annahmen

$$s = 7, \; 11, \; 13.$$

Dem zu Folge wird in allen 3 Fällen

$$z = x_0 - x_1 + x_2 \dots\dots + (-1)^m x_m$$

und die Theilbarkeit der Z durch eine unserer drei Zahlen s wird davon abhangen, ob es z ist. Offenbar erhalten wir die x, wenn wir den

dekadischen Zahlenausdruck für Z von der Rechten zur Linken in Klassen zu 3 Ziffern theilen und es ergiebt sich nun der Satz:

Eine Zahl ist durch eine der Primzahlen 7, 11, 13 theilbar, je nachdem es die Differenz ist, welche man erhält, wenn man die Summe der geraden dreiziffrigen Klassen abzieht von der Summe der ungeraden dreiziffrigen Klassen. Uebrigens lässt auch hier die Zahl denselben Rest, wie die erwähnte Differenz.

3) Theilbarkeit durch 27 und 37. Da $27 . 37 = 999$ ist, so wird jede der Annahmen

$$s = 27,\ 37$$

die Gleichung $nA = qs + r$ befriedigen, sobald man

$$n = 1,\ A = 100,\ r = +1$$

setzt und es folgt daher

$$z = x_0 + x_1 + x_2 + \ldots + x_m$$

Also, da x_0, x_1, ... wiederum die oben erwähnten dreiziffrigen Klassen bezeichnen: Eine Zahl ist durch 27 oder 37 theilbar, je nachdem es die Summe ihrer Klassen zu drei Ziffern ist; ist sie nicht durch eine dieser Zahlen theilbar, so lässt doch wenigstens diese Summe denselben Rest, wie die Zahl. Sei z. B.

$$Z = 25|084|365|147,$$

so wäre

$$z = 147 + 365 + 84 + 25 = 621;$$

diese Zahl ist aber durch 27 theilbar und lässt durch 37 dividirt den Rest 29; mithin ist gleichfalls Z durch 27 ohne Rest dividirbar und lässt durch 37 dividirt den Rest 29.

4) Theilbarkeit durch 9 und 11. Da $9.11 = 100 - 1$, setze man

$$A = 100,\ n = 1,\ r = -1,$$

so wird

$$z = x_0 - x_1 + x_2 + x_3 + \ldots + (-1)^m x_m$$

und mithin folgt der Satz: Eine Zahl ist durch 9 oder 11 theilbar, je nachdem es die Differenz ist, welche man erhält, wenn man die Summe ihrer geraden Klassen zu je zwei Ziffern abzieht von der Summe ihrer ungeraden Klassen zu zwei Ziffern. Eben so leicht, da $1. 10 = 1. 11 - 1$, bekommt man

den Satz: **Eine Zahl ist durch 11 theilbar, wenn es die Differenz ist, welche man erhält, wenn man die Summe ihrer geraden Ziffern abzieht von der Summe ihrer ungeraden Ziffern.**

5) **Theilbarkeit durch 17.** Man setze

$$A = 10,\ n = 5,\ r = -1,\ s = 17;$$

alsdann folgt

$$(-1)^m z = x_m - 5x_{m-1} + 25x_{m-2} - 125x_{m-3} + \ldots$$

und, wenn man die Vielfachen von 17 absondert, muss demgemäss Z durch 17 theilbar sein, wenn es der Ausdruck

$$x_m - 5x_{m-1} + 8x_{m-2} - 6x_{m-3} - 4x_{m-4} + 3x_{m-5} + 2x_{m-6}$$
$$+ 7x_{m-7} - x_{m-8} + 5x_{m-9} - 8x_{m-10} + \ldots\ldots$$

ist, wo $x_0, x_1, x_2, \ldots. x_m$ die dekadischen Ziffern der Zahl Z von der Rechten nach der Linken hin bezeichnen.

6) Wenn man in unserem allgemeinen Theoreme $n = 1$ setzt und $A = 10$, so bedeuten die x geradezu die aufeinander folgenden Ziffern der dekadischen Zahl z und die Bestimmung des Restes, welchen ihre Division mit irgend einer Primzahl s giebt, wird erhalten, indem man den Rest von z bestimmt. Dieser Rest wird aber nicht verändert, wenn man in den einzelnen Gliedern, aus denen z besteht, alle Vielfachen von s wegwirft und zwar wo möglich immer **das zunächst liegende** Vielfache, mag es nun unter oder über dem Werthe des betrachteten Gliedes liegen. Hierdurch erhält man an Stelle der ursprünglichen Form

$$z = x_0 + x_1 . r + x_2 . r^2 + x_3 . r^3 + \ldots.$$

eine einfachere

$$z = x_0 + ax_1 + bx_2 + cx_3 + \ldots\ldots,$$

wo $a, b, c, \ldots\ldots$ lauter entweder positive oder negative ganze Zahlen $< \frac{s}{2}$ bezeichnen. Man kann aber noch einen Schritt weiter gehen; denn die x können hier überall nur eine beschränkte Anzahl von Werthen erhalten, nämlich alle Werthe zwischen 0 und 10, und man kann sich daher eine Tabelle berechnen, in welcher für jeden dieser Werthe des betrachteten x die Restzahl verzeichnet steht, welche das bezügliche Glied nach Abwerfung aller ganzen Vielfachen von s übrig lässt. Aus dieser Tabelle

nun entnimmt man die den einzelnen Ziffern einer gegebenen Zahl entsprechenden Summanden, deren Summe denselben Rest lässt wie die Zahl selbst. Es möge eine Tabelle dieser Art für die Primzahlen 17, 19 folgen.

Tabelle für die Primzahl 17 ($r = -7$).

$$z = x_0 - 7x_1 - 2x_2 - 3x_3 + 4x_4 + 6x_5 - 8x_6 + 5x_7 - x_8 + 7x_9 + \ldots$$

Stellenzahl	Werth der Ziffern								
	1	2	3	4	5	6	7	8	9
1	+1	+2	+3	+4	+5	+6	+7	+8	−8
2	−7	+3	−4	+6	−1	−8	+2	−5	+5
3	−2	−4	−6	−8	+7	+5	+3	+1	−1
4	−3	−6	+8	+5	+2	−1	−4	−7	+7
5	+4	+8	−5	−1	+3	+7	−6	−2	+2
6	+6	−5	+1	+7	−4	+2	+8	−3	+3
7	−8	+1	−7	+2	−6	+3	−5	+4	−4
8	+5	−7	−2	+3	+8	−4	+1	+6	−6
9	−1	−2	−3	−4	−5	−6	−7	−8	+8
10	+7	−3	+4	−6	+1	+8	−2	+5	−5

Tabelle für die Primzahl 19 ($r = -9$).

$$z = x_0 - 9x_1 + 5x_2 - 7x_3 + 6x_4 + 3x_5 - 8x_6 - 4x_7 - 2x_8 - x_9 + 9x_{10} - \ldots$$

Stellenzahl	Werth der Ziffern								
	1	2	3	4	5	6	7	8	9
1	+1	+2	+3	+4	+5	+6	+7	+8	+9
2	−9	+1	−8	+2	−7	+3	−6	+4	−5
3	+5	−9	−4	+1	+6	−8	−3	+2	+7
4	−7	+5	−2	−9	+3	−4	+8	+1	−6
5	+6	−7	−1	+5	−8	−2	+4	−9	−3
6	+3	+6	+9	−7	−4	−1	+2	+5	+8
7	−8	+3	−5	+6	−2	+9	+1	−7	+4
8	−4	−8	+7	+3	−1	−5	−9	+6	+2
9	−2	−4	−6	−8	+9	+7	+5	+3	+1
10	−1	−2	−3	−4	−5	−6	−7	−8	−9

Es ist für den Anfänger gut, um sich an eine solche Betrachtungsweise der Division zu gewöhnen, bei welcher die Reste wesentlich ins Auge gefasst werden, den Bildungsgang einer solchen Tabelle näher zu verfolgen. So z. B. ist für $s = 17$ ursprünglich

$$z = x_0 + x_1 \cdot (-7) + x_2 \cdot (-7)^2 + x_3 \cdot (-7)^3 + \ldots;$$

aber es ist, wenn blos die Reste betrachtet werden,

$$
\begin{array}{llll}
-7 & \text{gleichbedeutend mit} & & -7 \\
(-7)^2 & \text{"} & \text{"} & -7.-7=3.17-2 \text{ oder } -2 \\
(-7)^3 & \text{"} & \text{"} & -2.-7=17-3 \text{ oder } -3 \\
(-7)^4 & \text{"} & \text{"} & -3.-7=17-4 \text{ oder } +4 \\
(-7)^5 & \text{"} & \text{"} & +4.-7=-34+6 \text{ oder} +6 \\
\end{array}
$$

. . . . . .

und ebenso hat man, was die Bildung z. B. der zweiten Horizontalreihe betrifft,

$$-7=-7,$$

$$-7+(-7)=-17+3 \text{ gleichbedeutend mit } +3,$$

$$+3+(-7)=-4,$$

$$-4+(-7)=-17+6 \text{ gleichbedeutend mit} +6,$$

. . . . . .

. . . . . .

Der Gebrauch, der von einer solchen Tabelle zu machen ist, ergiebt sich leicht. Z. B. es soll der Rest von

$$Z=80739$$

durch die Divisoren 17 und 19 untersucht werden. Die erste Stelle 9 von der Rechten zur Linken giebt in Betreff der Primzahl 17 den Rest -8, die zweite Stelle 3 den Rest -4, die dritte 7 den Rest $+3$, die vierte 0 den Rest 0, die fünfte 8 den Rest -2, also ist der Gesammtrest

$$-8-4+3-2=-11=-17+6 \text{ oder} +6$$

und in der That ist

$$\frac{80739}{17}=4749\frac{6}{17}.$$

Aehnlich ergiebt sich für die Primzahl 19 der Gesammtrest

$$+9-8-3-9=-11=-19+8 \text{ oder } +8;$$

also lässt 80739 durch 19 dividirt den Rest $+8$.

§. 3.

Wir wollen als Einleitung noch einige sehr allgemeine Sätze über relative Primzahlen vorausschicken, d. h. nach dem üblichen Sprachgebrauche über solche ganze Zahlen, die ausser der Einheit keinen gemein-

schaftlichen Theiler besitzen. Hierbei wollen wir grösserer Kürze halber die Anzahl aller Faktoren einer Zahl, die Einheit und sie selbst mit gezählt, durch S' bezeichnen, ferner die Summe aller dieser Faktoren mit S'' und endlich die Anzahl aller Zahlen, die kleiner als die betrachtete Zahl und relative Primzahlen zu ihr sind (die Einheit zählt wiederum mit), mit S''' bezeichnen. Mithin wird z. B. für die Zahl 12

$$S'\,12 = 6.$$
$$S''\,12 = 1 + 2 + 3 + 4 + 6 + 12 = 28.$$
$$S'''\,12 = 4.$$

Dieses vorausgesetzt kann man folgenden allgemeinen Satz aussprechen: Wenn M und N relative Primzahlen sind und man bestimmt sich für jede dieser Zahlen die verschiedenen S, so gilt für jedes die Relation:

$$SM.\ SN = S\,(MN).$$

Seien also $a, b, c, \ldots\ldots p, r, s, \ldots\ldots$ von einander verschiedene Primfaktoren und

$$M = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots;\ N = p^{\pi}\, r^{\varrho}\, s^{\sigma} \ldots\ldots,$$

so ist klar, dass man, um alle möglichen Faktoren von M zu erhalten, sich alle möglichen Combinationen der Elemente

$$1,\ a,\ a^2,\ a^3,\ \ldots\ldots\ a^{\alpha}$$
$$1,\ b,\ b^2,\ b^3,\ \ldots\ldots\ b^{\beta}$$
$$1,\ c,\ c^2,\ c^3,\ \ldots\ldots\ c^{\gamma}$$

deren Anzahl in den respektiven Horizontalreihen gleich $\alpha+1$, $\beta+1$, $\gamma+1$, ... ist, zusammensetzen muss und dass man alle diese Combinationen als Elemente einer Summe erhalten kann, wenn man das Produkt aller der Summenreihen sich bildet, welche aus der Summation der Elemente in einer solchen Horizontalreihe hervorgehen. Dies Produkt hat nun $(\alpha+1)(\beta+1)(\gamma+1)\ldots$ Glieder und eben diese Zahl giebt mithin die Anzahl der sämmtlichen Divisoren, welche M besitzt. Demgemäss folgt

$$S'M = (\alpha+1)(\beta+1)(\gamma+1)\ldots\ldots$$
$$S'N = (\pi+1)(\varrho+1)(\sigma+1)\ldots\ldots$$

und durch Multiplikation dieser beiden Gleichungen

$$S'M.S'N = (\alpha+1)(\beta+1)(\gamma+1)\ldots\ldots(\pi+1)(\varrho+1)(\sigma+1)\ldots\ldots,$$
$$= S'(MN),$$

wie zu erweisen war.

Man sieht ohne Weiteres ein, dass dieser Schluss nur dann Geltung habe, wenn die Primfaktoren von M andere sind, als die Primfaktoren von N; denn wenn z. B. a und p einander gleich wären, so würden in der Summe, deren Elemente die Divisoren von MN sind, mehrere Glieder als verschieden gezählt sein, die doch nur dieselben Potenzen von a vorstellen, und die Anzahl der Divisoren wäre hiernach grösser, als sie es wirklich ist. Der Satz gilt also nur für relative Primzahlen.

Wenn ferner das Zeichen S die Summe der Faktoren bedeutet, so ist

$$S''M=(1+a+a^2+\ldots+a^\alpha)(1+b+b^2+\ldots+b^\beta)(1+c+c^2+\ldots+c^\gamma)\ldots$$

oder, da jeder Faktor eine geometrische Progression bildet, nach der bekannten Summenformel für eine derartige Reihe

$$=\frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\cdot\frac{c^{\gamma+1}-1}{c-1}\cdots\cdot$$

Ganz ebenso entwickelt man sich

$$S''N=\frac{p^{\pi+1}-1}{p-1}\cdot\frac{r^{\varrho+1}-1}{r-1}\cdot\frac{s^{\sigma+1}-1}{s-1}\cdots,$$

mithin

$$S''M\,.\,S''N=\frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\cdots\frac{p^{\pi+1}-1}{p-1}\cdot\frac{r^{\varrho+1}-1}{r-1}\cdots$$
$$=S''(MN).$$

Es bleibt nur noch übrig zu beweisen, dass unser Gesetz auch dann noch Geltung hat, wenn S die Anzahl aller Zahlen bezeichnet, die kleiner als eine gegebene Zahl und relative Primzahlen zu dieser nämlichen Zahl sind. Die Gesammtheit dieser Zahlen für irgend eine gegebene Zahl M wird erhalten, wenn man aus der Reihe der Zahlen von 1 bis M alle diejenigen ausschliesst, welche einen gemeinsamen Theiler mit M haben. Nun sind zunächst diejenigen Zahlen, welche einen Theiler a mit M gemeinschaftlich besitzen,

$$a\ 2a\ 3a\ 4a\ \ldots\ \frac{M}{a}a$$

und ihre Anzahl offenbar $\frac{M}{a}$, mithin die Gesammtheit der durch a nicht theilbaren Zahlen die Menge der übrig bleibenden aus der Zahlenreihe von 1 bis M, nämlich

$$M-\frac{M}{a}=M\left(1-\frac{1}{a}\right).$$

Die durch b theilbaren Zahlen von 1 bis M sind

$$b \quad 2b \quad 3b \quad 4b \; \ldots\ldots \; \frac{M}{b} \cdot b$$

und ihre Anzahl $\frac{M}{b}$. Nun können aber doch unter diesen auch solche sein, die ausser durch b auch noch durch a theilbar und demgemäss schon in Rechnung gebracht sind. Die Reihe dieser Zahlen ist

$$ab \quad 2ab \quad 3ab \; \ldots\ldots \; \frac{M}{ab} \cdot ab$$

und ihre Anzahl $\frac{M}{ab}$. Mithin ist die Anzahl der Zahlen, welche durch b theilbar sind, ohne es gleichzeitig durch a zu sein

$$\frac{M}{b} - \frac{M}{ab} = \frac{M}{b}\left(1 - \frac{1}{a}\right)$$

und wir erhalten dem zu Folge als die Anzahl der Zahlen von 1 bis M, welche weder durch a noch durch b theilbar sind

$$M\left(1 - \frac{1}{a}\right) - \frac{M}{1}\left(1 - \frac{1}{a}\right) = M\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right).$$

Ganz in derselben Weise können wir weiter gehen. Die Anzahl der von 1 bis M durch c theilbaren Zahlen ist $\frac{M}{c}$, hier sind aber diejenigen mitgezählt, die zu gleicher Zeit durch einen der Faktoren a, b, ab theilbar sind und schon anderweitig in Rechnung gezogen wurden, nämlich

$$ac, \; 2ac, \; 3ac, \; \ldots\ldots \; \frac{M}{ac}\, ac,$$

$$bc, \; 2bc, \; 3bc, \; \ldots\ldots \; \frac{M}{bc}\, bc,$$

$$abc, \; 2abc, \; 3abc, \; \ldots\ldots \; \frac{M}{abc}\, abc,$$

Die Anzahl dieser letzteren Zahlen ist, in Rücksicht dessen, dass die den beiden ersten Reihen gemeinschaftlich zukommenden Glieder die dritte Reihe ausmachen,

$$\frac{M}{ac} + \frac{M}{bc} - \frac{M}{abc}.$$

Mithin ist die Anzahl derjenigen Glieder der Reihe

$$c \quad 2c \quad 3c \; \ldots\ldots \; \frac{M}{c},$$

welche in den vorhin betrachteten Reihen nicht enthalten sind,

$$\frac{M}{c}-\frac{M}{ac}-\frac{M}{bc}+\frac{M}{abc}=\frac{M}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$$

und schliesslich die Anzahl aller weder durch a, noch durch b, noch durch c theilbaren Zahlen von 1 bis M

$$M\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)-\frac{M}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)=M\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right).$$

Dies Beweisverfahren lässt sich bei grösserer Anzahl der Primfaktoren beliebig weit fortsetzen und es darf daher geschlossen werden:

$$S'''M=M\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\ldots,$$

$$S'''N=N\left(1-\frac{1}{p}\right)\left(1-\frac{1}{r}\right)\left(1-\frac{1}{s}\right)\ldots\ldots,$$

woher durch Multiplikation

$$S'''M\,.\,S'''N=MN\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots\ldots\left(1-\frac{1}{p}\right)\left(1-\frac{1}{r}\right)\ldots\ldots$$
$$=S'''(MN).$$

Natürlich gilt auch hier die bereits oben auseinandergesetzte beschränkende Bestimmung, dass M und N relative Primzahlen sind. Denn hätten sie z. B. einen Primfaktor gemeinschaftlich, etwa $a=p$, so fielen die wegen der Theilbarkeit durch a und p ausgeschlossenen Zahlen von 1 bis MN zusammen, trotzdem dass sie zweimal in Anrechnung gebracht sind.

Weiter führen wir folgende Sätze auf:

Wenn $A<M$ und beide relative Primzahlen zu einander sind, so ist auch $M-A$ eine relative Primzahl zu M.

Die Anzahl der relativen Primzahlen zu M, welche kleiner als M sind, muss stets eine gerade sein. (Ausgenommen ist nur die Zahl 2).

Was den ersten Satz anbetrifft, so folgt er aus der einfachen Bemerkung, dass, wenn $M-A$ und M einen gemeinschaftlichen Faktor hätten, derselbe nothwendig auch ein Faktor von A sein müsste, gegen die Voraussetzung, nach der A und M keinen gemeinschaftlichen Faktor haben. Der zweite Satz folgt unmittelbar aus dem ersten, dem zu Folge zu jeder relativen Primzahl $<\frac{1}{2}M$ eine relative Primzahl zwischen $\frac{1}{2}M$ und M gehören muss.

Eine interessante Folgerung aus dem Vorigen ist der Satz:

Wenn man alle Theiler einer Zahl sucht, die Einheit und die Zahl selbst mit gerechnet, und für jeden dieser Theiler die Anzahl aller relativen Primzahlen, die kleiner sind, als er selbst, sich bestimmt, so ist die Summe aller dieser S''' der Zahl selber gleich.

Wenn $1, \mu, \mu', \mu'', \ldots\ldots n$ die sämmtlichen Theiler einer Zahl sind, so ist der analytische Ausdruck des ausgesprochenen Satzes:

$$1 + S'''\mu + S'''\mu' + S'''\mu'' + \ldots. + S'''n = n.$$

Sei z. B. $n = 20$, so sind die einzelnen Theiler dieser Zahl der Reihe nach

$$1,\ 2,\ 4,\ 5,\ 10,\ 20$$

und man hat

$$S'''1 = 1,\ S'''2 = 1,\ S'''4 = 2,\ S'''4 = 2,\ S'''5 = 4,$$
$$S'''10 = 4,\ S'''20 = 8.$$

Summirt man diese verschiedenen S''', so bekommt man in der That

$$1 + 1 + 2 + 4 + 4 + 8 = 20.$$

Um den Satz zu beweisen, nehmen wir zuerst den speciellen Fall vor, in welchem

$$M = a^{\alpha}$$

die Potenz einer einzigen Primzahl ist und mithin die Reihe der Theiler mit der Progression

$$1\ a\ a^2\ a^3\ \ldots.\ a^{\alpha}$$

zusammenfällt. Nun geht aber aus den vorhergehenden Betrachtungen hervor, dass wenn a^{β} eine beliebige Potenz der Primzahl a bezeichnet

$$S'''a^{\beta} = a^{\beta}\left(1 - \frac{1}{a}\right) = a^{\beta-1}(a-1)$$

wird; mithin folgt

$$S'''1 + S'''a + S'''a^2 + S'''a^3 + \ldots. + S'''a^{\alpha}$$
$$= 1 + a - 1 + a(a-1) + a^2(a-1) + \ldots. + a^{\alpha-1}(a 1)$$
$$= 1 + (a-1)\left(1 + a + a^2 \ldots\ldots + a^{\alpha-1}\right)$$

oder da die eingeklammerte Progression den Ausdruck

$$\frac{a^{\alpha}-1}{a-1}$$

zur Summe hat

$$= 1 + a - 1 \cdot \frac{a^\alpha - 1}{a - 1} = a^\alpha,$$

und dieses war eben zu beweisen.

Sei nun M irgend wie zusammengesetzt, also

$$M = a^\alpha b^\beta c^\gamma \ldots\ldots\ldots,$$

so liefert uns die Entwickelung des Produktes

$$(1 + a + a^2 + \ldots + a^\alpha)(1 + b + b^2 + \ldots + b^\beta)(1 + c + c^2 + \ldots + c^\gamma) \ldots$$

die sämmtlichen Theiler der gegebenen Zahl als Elemente einer Summe. In dieser Summenreihe müssen wir an Stelle jedes Elementes das bezügliche S''' treten lassen und den dadurch entstehenden Reihenausdruck summiren. Da aber das S''' eines Produktes durch das Produkt aus den S''' der einzelnen Faktoren ersetzt werden kann, so kann man einfacher schon vor Ausführung der Multiplikation jedes einzelne Glied irgend eines Faktors durch sein S''' ersetzen. Die in Frage stehende Summe wird mithin gleich

$$(S'''1 + S'''a + \ldots + S'''a^\alpha)(S'''1 + S'''b + \ldots + S'''b^\beta)(S'''1 + S'''c + \ldots + S'''c^\gamma) \ldots$$

Die einzelnen Faktoren dieses Produktes geben nach dem eben bewiesenen speciellen Falle respective a^α, b^β, c^γ, ... und wir bekommen also schliesslich, in Uebereinstimmung mit dem ausgesprochenen Theoreme

$$a^\alpha b^\beta c^\gamma \ldots\ldots = M.$$

Eine äusserst interessante Bemerkung in Bezug auf das S'' hat Euler gemacht. Nehmen wir alle Zahlen in ihrer natürlichen Reihenfolge und entwickeln uns das S'' rücksichtlich jeder, so erhalten wir für die Zahlen von 1 bis 100 folgende Tabelle, in welcher rechts neben jeder Zahl das zugehörige S'' sich verzeichnet findet:

M	$S''M$	M	$S''M$	M	$S''M$	M	$S''M$	M	$S''M$
1	1	9	13	17	18	25	31	33	48
2	3	10	18	18	39	26	42	34	54
3	4	11	12	19	20	27	40	35	48
4	7	12	28	20	42	28	56	36	91
5	6	13	14	21	32	29	30	37	38
6	12	14	24	22	36	30	72	38	60
7	8	15	24	23	24	31	32	39	56
8	15	16	31	24	60	32	63	40	90

M	S''M	M	S''M	M	S''M	M	S''M	M	M
41	42	53	54	65	84	77	96	89	90
42	96	54	120	66	144	78	168	90	234
43	44	55	72	67	68	79	80	91	112
44	84	56	120	68	126	80	186	92	168
45	78	57	80	69	96	81	121	93	128
46	72	58	90	70	144	82	126	94	144
47	48	59	60	71	72	83	84	95	120
48	124	60	168	72	195	84	224	96	252
49	57	61	62	73	74	85	108	97	98
50	93	62	96	74	114	86	132	98	171
51	72	63	104	75	124	87	120	99	156
52	98	64	127	76	140	88	180	100	217

Obgleich in diesen Zahlen kein Gesetz enthalten zu sein scheint, sondern Primzahlen und zusammengesetzte Zahlen mit einander abwechseln, so muss man um so mehr den erhabenen Geist Eulers bewundern, der dennoch ein Gesetz zu entdecken wusste, und zwar fand er hierin einen Zusammenhang mit den Pentagonalzahlen, mit welchen diese auch nicht die entfernteste Aehnlichkeit zu haben scheinen.

Die $p$eckigen Zahlen sind bekanntlich aus einer solchen gewöhnlichen arithmetischen Progression entstanden, deren Anfangsglied 1 und deren Differenz $p-2$ ist; also liegt den Pentagonalzahlen die Reihe

$$1 \quad 4 \quad 7 \quad 10 \quad 13 \quad 16 \quad 19 \ldots\ldots$$

zu Grunde, und um sie zu erhalten muss man sich nach einander die Summe der 1, 2, 3, 4 ..... ersten Glieder der vorstehenden Reihe bilden. Die Pentagonalzahlen sind demgemäss

$$1 \quad 5 \quad 12 \quad 22 \quad 35 \quad 51 \quad 70 \ldots.$$

Nun hindert aber nichts, dass wir die Bildung dieser Reihen uns auch von der Rechten nach der Linken fortgesetzt denken, so dass wir negative Glieder bekommen, und man sieht augenblicklich ein, wie, um irgend eine Pentagonalzahl in dieser Art rückwärts zu bilden, man nur die nächst höhere um das gleich hohe Glied der darüber stehenden zu vermindern hat. Zu Folge dieser Bemerkung liefert uns die Stammreihe

$$\ldots. -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19, \ldots.$$

die Reihe

$$\ldots\ldots.\ 26,\ 15,\ 7,\ 2,\ 0,\ 1,\ 5,\ 12,\ 22,\ 35,\ 51,\ 70,\ \ldots.$$

oder, indem wir die einzelnen Glieder nach ihrer absoluten Grösse ordnen:

$$0,\ 1,\ 2,\ 5,\ 7,\ 12,\ 15,\ 22,\ 26,\ 35,\ 40,\ 51,\ \ldots.$$

und in diesem erweiterten Sinne wollen wir im Folgenden die Pentagonalzahlen nehmen. Dieses vorausgesetzt hat Euler bewiesen, dass

$$\begin{aligned} 0 = S''n - S''(n-1) - S''(n-2) + S''(n-5) + S''(n-7) \\ - S''(n-12) - S''(n-15) + S''(n-22) + S''(n-26) \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{aligned}$$

und mithin die Theilersumme einer Zahl n vermittelst der Pentagonalzahlen recurrirend dargestellt werden könne. Die Reihe muss fortgesetzt werden, so lange man unter dem Zeichen S'' noch eine positive ganze Zahl hat, die 0 als solche mit eingerechnet; wenn sie indessen mit $S''0$ schliessen sollte, ein Fall, der immer eintrifft, sobald n selber eine Pentagonalzahl ist, muss man für diesen Term, damit die Gleichung Bestand habe, die Zahl n selbst einsetzen. Setzt man z. B. $n = 15$, so soll sein

$$S''15 - S''14 - S''13 + S''10 + S''8 - S''3 - S''0 = 0$$

und, indem man die eben gemachte Bemerkung und die obige Tabelle anwendet, findet sich in der That

$$24 - 24 - 14 + 18 + 15 - 4 - 15 = 0.$$

Sei ferner $n = 21$, so soll sein

$$S''21 - S''20 - S''19 + S''16 + S''14 - S''7 - S''6 = 0$$

und es folgt aus der Tabelle in Uebereinstimmung hiermit

$$32 - 42 - 20 + 31 + 24 - 8 - 12 = 0.$$

Um diesen Satz zu beweisen, gehen wir mit Euler davon aus, dass man dem Produkte

$$(1+a)(1+b)(1+c)(1+d)\ldots.$$

die Form

$$1 + a + b(1+a) + c(1+a)(1+b) + d(1+a)(1+b)(1+c) + \ldots..$$

geben kann. Setzen wir nun, unter der Voraussetzung, dass

$$a = -x,\ b = -x^2,\ c = -x^3,\ d = -x^4,\ \ldots.$$

sei, den Werth dieses Produktes gleich s, so haben wir

$$\begin{aligned} s = (1-x)(1-x^2)(1-x^3)(1-x^4)\ldots. = 1 - x - x^2(1-x) \\ - x^3(1-x)(1-x^2) - x^4(1-x)(1-x^2)(1-x^3) - \ldots. \end{aligned}$$

In Analogie hiermit soll weiter sein:

$$s' = 1 - x + x(1-x)(1-x^2) + x^2(1-x)(1-x^2)(1-x^3) + \ldots.$$
$$s'' = 1 - x^2 + x^2(1-x^2)(1-x^3) + x^4(1-x^2)(1-x^3)(1-x^4) + \ldots.$$

. . . . . .

. . . . . .

$$s^{(n)} = 1 - x^n + x^n(1-x^n)(1-x^{n+1}) + x^{2n}(1-x^n)(1-x^{n+1})(1-x^{n+2}) + \ldots$$
$$s^{(n+1)} = 1-x^{n+1}+x^{n+1}(1-x^{n+1})(1-x^{n+2})+x^{2n+2}(1-x^{n+1})(1-x^{n+2})(1-x^{n+3})+\ldots.$$

Der Reihe $s^{(n)}$ können wir aber leicht folgende Form geben (durch Herausziehung von $1 - x^n$):

$$s^{(n)} = \left\{1 + x^n(1-x^{n+1}) + x^{2n}(1-x^{n+1})(1-x^{n+2}) + \ldots.\right\}(1-x^n)$$
$$= 1 + x^n(1-x^{n+1}) + x^{2n}(1-x^{n+1})(1-x^{n+2}) + \ldots.$$
$$- x^n \qquad - x^{2n}(1-x^{n+1}) \qquad - \ldots.$$
$$= 1 - x^{2n+1} - x^{3n+2}(1-x^{n+1}) - x^{4n+3}(1-x^{n+1})(1-x^{n+2}) - \ldots.$$
$$= 1 - x^{2n+1} - x^{3n+2}\left\{1 - x^{n+1} + x^{n+1}(1-x^{n+1})(1-x^{n+2}) + \ldots.\right\},$$

Betrachten wir die Parenthese, so erkennen wir, dass sie nichts anderes als die Reihe $s^{(n+1)}$ ist und es ergiebt sich daher folgende Recursionsformel für die s:

$$s^{(n)} = 1 - x^{2n+1} - x^{3n+1} s^{(n+1)}.$$

Diese Formel begreift auch selbst unser ursprüngliches s in sich, wofern man in ihr $n = 0$ und $s^{(0)} = s$ annimmt, wie man sich durch eine Betrachtung der Reihenausdrücke für s und s' leicht überzeugen kann, und man erhält demgemäss, indem man der Reihe nach $n = 0, 1, 2, 3, \ldots.$ einsetzt,

$$s = 1 - x - x^2 s',$$
$$s' = 1 - x^3 - x^5 s'',$$
$$s'' = 1 - x^5 - x^8 s'''$$
$$s''' = 1 - x^7 - x^{11} s^{IV},$$
$$s^{IV} = 1 - x^9 - x^{14} s^{V}$$

. . . . . .

. . . . . .

Setzen wir diese Werthe allmählig in einander ein, so ergiebt sich

$$s = 1 - x - x^2(1-x^3) + x^{2+5}(1-x^5) - x^{2+5+8}(1-x^7) + x^{2+5+8+11}(1-x^9) - \ldots.$$

also wenn man die Rechnung rechts ausführt und für s seinen Werth einsetzt:

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\ldots\ldots$$
$$= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - \ldots.$$

und auf der rechten Seite dieser Gleichung springt sogleich in die Augen, dass die aufeinander folgenden Exponenten von x weiter nichts sind, als die Pentagonalzahlen nach ihrer absoluten Grösse geordnet.

Logarithmiren wir jetzt die Gleichung

$$s = (1-x)(1-x^2)(1-x^3)\ldots.$$

auf beiden Seiten, so folgt

$$lgs = lg(1-x) + lg(1-x^2) + lg(1-x^3) + \ldots.$$

und wenn wir die bekannte Reihe

$$lg(1-a) = -\frac{a}{1} - \frac{a^2}{2} - \frac{a^3}{3} - \frac{a^4}{4} - \ldots.$$

nach einander für

$$a = -x,\ -x^2,\ -x^3,\ \ldots.$$

benutzen:

$$\begin{array}{rcccccccccl}
-lgs = & \frac{x}{1} & +\frac{x^2}{2} & +\frac{x^3}{3} & +\frac{x^4}{4} & +\frac{x^5}{5} & +\frac{x^6}{6} & +\frac{x^7}{7} & +\frac{x^8}{8} & +\frac{x^9}{9} & +\ldots. \\
 & & +\frac{x^2}{1} & & +\frac{x^4}{2} & & +\frac{x^6}{3} & & +\frac{x^8}{4} & & +\ldots. \\
 & & & +\frac{x^3}{1} & & & +\frac{x^6}{2} & & & +\frac{x^9}{3} & +\ldots. \\
 & & & & +\frac{x^4}{1} & & & & +\frac{x^8}{2} & & +\ldots. \\
 & & & & & +\frac{x^5}{1} & & & & & +\ldots. \\
 & & & & & & +\frac{x^6}{1} & & & & +\ldots. \\
 & & & & & & & +\frac{x^7}{1} & & & +\ldots. \\
 & & & & & & & & +\frac{x^8}{1} & & +\ldots. \\
 & & & & & & & & & +\frac{x^9}{1} & +\ldots.
\end{array}$$

Betrachten wir diese Entwickelung, so gehen doch alle Horizontalreihen aus der ersten hervor, wenn man successive $= x^2, x^3, x^4, \ldots.$ für x einsetzt; mithin sind die aufeinander folgenden Exponenten von x in ihnen respektive die Vielfachen der Zahlen 2, 3, 4, 5, ... In Rücksicht darauf ergiebt sich leicht, dass der Coefficient von x^n die Summe aller Brüche

sein wird, deren Zähler 1 ist und deren Nenner alle nur möglichen Theiler von n sind. So z. B. ist der Coefficient von x^6 gleich $\frac{1}{6}+\frac{1}{3}+\frac{1}{2}+\frac{1}{1}$, von x^8 gleich $\frac{1}{8}+\frac{1}{4}+\frac{1}{2}+\frac{1}{1}$. Allgemein seien die Theiler einer beliebigen Zahl n der Reihe nach $1, n', n'', n''', \ldots\, n$ und ein beliebiger darunter $n^{(\mu)}$: so wird in der ersten Horizontalreihe nothwendig einmal das Glied $\frac{x^{n^{(\mu)}}}{n^{(\mu)}}$ vorkommen müssen, weil in derselben die Exponenten weiter nichts sind, als die Zahlen in ihrer natürlichen Aufeinanderfolge; aus ähnlichen Gründen wird unter den Ausdrücken $lg(1-x)$, $lg(1-x^2)$, ... einer, nämlich $lg\left(1-x^{\frac{n}{n^{(\mu)}}}\right)$, vorkommen, welcher sich auf die $\frac{n}{n^{(\mu)}}$te Potenz von x bezieht, und das oben erwähnte Glied der ersten Horizontalreihe giebt in der Entwickelung des letztgenannten Logarithmus den Term:

$$\frac{\left(x^{\frac{n}{n^{(\mu)}}}\right)^{n^{(\mu)}}}{n^{(\mu)}} = \frac{x^n}{n^{(\mu)}}$$

und es kommt also wirklich jeder beliebige Bruch von der Form $\frac{1}{n^{(\mu)}}$ als Coefficient der $n$ten Potenz von x vor. Addirt man daher zusammen, so ergiebt sich als der Coefficient von x^n nothwendig

$$\frac{1}{1}+\frac{1}{n'}+\frac{1}{n''}+\ldots+\frac{1}{n} = \frac{\frac{n}{1}+\frac{n}{n'}+\frac{n}{n''}+\ldots+\frac{n}{n}}{n}$$

$$= \frac{n+\ldots\ldots+n''+n'+1}{n}$$

$$= \frac{S''n}{n}$$

Unsere Reihe geht also einfach über in

$$-lgs = \frac{x}{1}S''1 + \frac{x^2}{2}S''2 + \frac{x^3}{3}S''3 + \frac{x^4}{4}S''4 + \frac{x^5}{5}S''5 + \ldots$$

und sie kann sogar noch mehr vereinfacht werden, wenn man die Gleichung erst nach x als der unabhängig Veränderlichen differentiirt und darauf mit x multiplizirt, wodurch

$$-\frac{x}{s}\frac{ds}{dx} = xS''1 + x^2S''2 + x^3S''3 + x^4S''4 + x^5S''5 + \ldots$$

wird. Vermöge des Reihenausdruckes

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \ldots.$$

erhält man aber mit Leichtigkeit eine zweite Reihe für dieselbe Quantität $-\frac{x}{s}\frac{ds}{dx}$. Zu diesem Zwecke hat man nur nöthig ihn erst nach x zu differentiiren und darauf mit

$$-\frac{x}{s} = -\frac{x}{1 - x - x^2 + x^5 + x^7 - \ldots..}$$

zu multipliziren. Hierdurch kommt

$$-\frac{x}{s}\frac{ds}{dx} = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \ldots.}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \ldots.}$$

und setzen wir jetzt beide Reihenausdrücke einander gleich, so ergiebt sich ohne Mühe, dass der Zähler des zweiten gleich ist dem Produkte aus dem ersten in den Nenner des zweiten, und durch Ausführung der Multiplikation:

$$\begin{aligned} x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \ldots. \\ = xS''1 + x^2S''2 + x^3S''3 + x^4S''4 + x^5S''5 + x^6S''6 + x^7S''7 + x^8S''8 + \ldots \\ - x^2S''1 - x^3S''2 - x^4S''3 - x^5S''4 - x^6S''5 - x^7S''6 - x^8S''7 - \ldots \\ - x^3S''1 - x^4S''2 - x^5S''3 - x^6S''4 - x^7S''5 - x^8S''6 - \ldots \\ + x^6S''1 + x^7S''2 + x^8S''3 - \ldots \\ + x^8S''1 + \ldots \end{aligned}$$

Das allgemeine Glied der zweiten Reihe ist leicht erkennbar und die Vergleichung der gleich hohen Coefficienten beider Reihen giebt nun augenblicklich

$$S''n - S''(n-1) - S''(n-2) + S''(n-5) + S''(n-7) - S''(n-12) - \ldots. = \begin{cases} 0 \text{ od.} \\ \pm n. \end{cases}$$

Das Erste wird im Allgemeinen immer statt finden, das zweite, wenn n selber eine Pentagonalzahl ist und also nach dem Gesetze der Rechenentwickelung auf der linken Seite daselbst als letztes Glied noch $+S''(n-n) = \pm S''0$ hinzutreten müsste — in Uebereinstimmung mit der Aussprache des Eulerschen Satzes.

Erster Abschnitt.

Von der Congruenz der Zahlen.

§. 4.

Indem wir jetzt auf unseren Gegenstand näher eingehen, haben wir zunächst den Begriff der Zahlencongruenzen zu erörtern, welcher zuerst von Gauss in die Wissenschaft eingeführt worden ist. Die Fundamentalerklärung lautet: Wenn die Differenz $(a-b)$ zweier Zahlen durch eine dritte Zahl c ohne Rest theilbar ist, so nennt man die beiden Zahlen a und b einander nach dem Modul c congruent, und bezeichnet dieses Verhältniss, wie folgt:

$$a \equiv b \ (mod\ c).$$

Legendre bedient sich in seiner Theorie der Zahlen zur Bezeichnung desselben Verhältnisses geradezu des Gleichheitszeichens, und das ist in der Natur der Untersuchung auch vollkommen begründet. Denn wenn $\frac{a-b}{c}$ ein ganzzahliger Ausdruck ist, so muss der gewöhnliche Divisionsrest der Quotienten $\frac{a}{c}$ und $\frac{b}{c}$ derselbe sein, und da es sich in der gesammten höheren Arithmetik wesentlich um die Reste handelt, so ist es erklärlich, wenn wir solche Zahlen, die durch irgend einen Modul dividirt denselben Rest lassen, als congruente Zahlen bezeichnen. Hiernach ist z. B.

$$27 \equiv 19 \quad (mod\ 4),$$

$$\left.\begin{array}{l} 27 \equiv 15 \\ 27 \equiv 11 \\ 27 \equiv \ \ 3 \end{array}\right\} (mod\ 4)$$

und in der letzten Gestalt haben wir geradezu die Zahl 27 als congruent ihrem gewöhnlichen Divisionsrest. Solche Zahlen dagegen, welche bei der Division durch einen und denselben Modul verschiedene Reste lassen, heissen

incongruent, und es sind daher z. B. die Zahlen 19 und 28 in Bezug auf den Modul 4 incongruent, dagegen in Bezug auf den Modul 3 congruent.

Wir müssen hieran noch gleich die Erklärung einer anderen Benennung anknüpfen, nämlich die Erklärung dessen, was wir im Folgenden unter dem kleinsten Reste verstehen. Wenn nämlich irgend eine Zahl durch einen beliebigen Divisor (den Modul) dividirt wird, so ist der kleinste Rest eine Zahl, die nach ihrer absoluten Grösse nicht grösser als der halbe Divisor ist. Es ist klar, dass bei Zulassung negativer Reste immer ein solcher Divisionsrest existirt. So z. B. lässt 38 bei der Division durch 5 allerdings den Rest 3, welcher grösser als $\frac{5}{2}$ ist, aber man braucht blos 38 sich unter der Form $5 \cdot 8 - 2$ zu denken und hat dann sofort den kleinsten Rest -2. Eine Zahl ist immer ihrem kleinsten Reste congruent, also z. B.:

$$38 \equiv -2 \pmod 5),$$

und in der That hat man, in Uebereinstimmung mit der Definition,

$$\frac{38-(-2)}{5} = \frac{38+2}{5} = \frac{40}{5} = 8.$$

Wir werden künftig in den meisten Fällen uns nur solcher kleinsten Reste bedienen und ein auf den Modul n bezüglicher kleinster Rest muss daher, wenn n eine ungerade Zahl bezeichnet, nothwendig mit einer der Zahlen

$$\frac{n-1}{2}, \frac{n-3}{2}, \frac{n-5}{2}, 1, 0, -1, \ldots. -\frac{n-5}{2}, -\frac{n-3}{2}, -\frac{n-1}{2}$$

zusammenfallen.

Aus dem Begriffe der Congruenz fliessen unmittelbar folgende Sätze:

1) Wenn zwei Zahlen b und d nach einem gewissen Modul c einer und derselben dritten Zahl congruent sind, so sind sie nach demselben Modul auch unter einander congruent. In Zeichen, wenn beidemal nach dem Modul c

$$a \equiv b \text{ und } a \equiv d,$$

so folgt

$$b \equiv d \pmod c).$$

3) Wenn wir die Congruenzen

$$a \equiv b \text{ und } d \equiv e \pmod c)$$

haben, so kann man (ganz so, als ob es Gleichungen wären) folgern:

$$a \mp d \equiv b \mp e \pmod{c}$$

und

$$ad \equiv be \pmod{c}.$$

Der Beweis des letzten Satzes ergiebt sich, wenn man bemerkt, dass zu Folge der Definition der Congruenz $\frac{a-b}{c}$ und $\frac{d-e}{c}$ ganze Zahlen sind, also etwa

$$\frac{a-b}{c} = m \; . \; \frac{d-e}{c} = n.$$

Hieraus folgt durch leichte algebraische Umformung

$$ad = c^2mn + c(me + nb) + be,$$

woher

$$\frac{ad - be}{c} = cmn + me + nb,$$

und da die rechte Seite hier offenbar ein ganzzahliger Ausdruck ist, so ist unsere Behauptung, dass ad und be einander congruent seien, gerechtfertigt.

Aus diesem Satze für die Multiplikation ergiebt sich sogleich der Satz für die Potenzirung, der jedoch nur unter der Voraussetzung ganzer positiver Exponenten gilt:

3) **Wenn zwei Zahlen nach einem gewissen Modul congruent sind, so sind ihre gleich hohen Potenzen nach demselben Modul congruent.** Z. B. es ist

$$9 \equiv 4 \pmod{5};$$

mithin

$$9^3 \equiv 4^3 \text{ oder } 729 \equiv 64 \pmod{5}.$$

Die Addition, Subtraction und Multiplication kann hiernach beliebig auf Congruenzen angewandt werden, in derselben Weise als ob sie geradezu Gleichungen wären. Bei der Division hingegen kann man das nicht ohne eine Einschränkung. Der bezügliche Satz lautet:

4) **Wenn a und b zu c relative Primzahlen sind und man hat**

$$\left.\begin{array}{l} a \equiv b \\ ad \equiv be \end{array}\right\} \pmod{c},$$

so folgt durch Division

$$d \equiv e \pmod{c}.$$

Zum Beweise bemerke man, dass aus der Congruenz $a \equiv b$ sich die Congruenz $ad \equiv bd$ ergiebt und mithin wegen der zweiten gegebenen Congruenz nach unserem ersten Satze $bd \equiv be$, oder

$$\frac{b(d-e)}{c} = Intg,$$

wo wir unter dem Zeichen $Intg$ eine beliebige ganze Zahl verstehen. Da nun b und c der Voraussetzung nach relative Primzahlen sind, so kann dieser Quotient nur dadurch eine ganze Zahl geben, dass $\frac{d-e}{c}$ einer ganzen Zahl gleich wird; die fragliche Congruenz ist hiermit gerechtfertigt.

Man kann einen ähnlichen Satz für die Multiplikation zweier Moduli aufstellen:

5) Wenn die Zahlen a und b einander gleichzeitig nach zwei relativen Primzahlen m und n congruent sind, so sind sie einander auch nach deren Produkte mn congruent. In Zeichen, wenn

$$a \equiv b \ (mod\ m) \text{ und } a \equiv b \ (mod\ n),$$

so folgt

$$a \equiv b \ (mod\ mn).$$

Der Satz ist identisch mit dem bekannten Satze: Wenn eine Zahl $a-b$ durch zwei relative Primzahlen theilbar ist, so ist sie auch durch deren Produkt theilbar.

6) Wenn zwei Zahlen nach dem Produkte zweier anderen congruent und beide durch den einen Faktor theilbar sind, so sind die Quotienten einander nach dem anderen Faktor congruent. In Zeichen, aus der Congruenz

$$a \equiv b \ (mod\ mn)$$

folgt, wenn $\frac{a}{n}$ und $\frac{b}{n}$ ganze Zahlen sind,

$$\frac{a}{n} \equiv \frac{b}{n} \ (mod\ m).$$

Es ergiebt sich dies leicht. Denn wenn $a-b$ durch mn theilbar ist, so muss diese Division auch aufgehen, wenn man erst mit n und darauf mit m dividirt. Das Resultat der ersten Division ist aber eine ganze Zahl, weil $a-b$ durch jeden Faktor von mn theilbar sein muss, also

$$\frac{a-b}{n} \equiv 0 \pmod{m},$$

und hieraus folgt unter der gemachten Voraussetzung, da

$$\frac{b}{n} \equiv \frac{b}{n} \pmod{m},$$

durch Addition dieser beiden Congruenzen

$$\frac{a}{n} \equiv \frac{b}{n} \pmod{m}.$$

Dieser Satz findet in Verbindung mit 4) häufige Anwendung.

Es sei z. B.

$$99 \equiv 27 \pmod{24},$$

so folgt nach ihm durch Division mit 3

$$33 \equiv 9 \pmod{8},$$

und hieraus nach 4) durch abermalige Division mit 3

$$11 \equiv 3 \pmod{8}.$$

§. 5.

Auf Grundlage der eben erörterten Principien können wir nun sogleich zur Betrachtung der unbestimmten Gleichungen des ersten Grades fortschreiten. Ehe wir jedoch das hierher gehörige Theorem, welches ein Fundamentalsatz der ganzen unbestimmten Analysis ist, beweisen, wollen wir folgenden Hilfssatz vorausschicken:

Wenn a und b relative Primzahlen zu einander sind und man dividirt die $(b-1)$ auf einander folgenden Vielfachen der einen Zahl a, nämlich

$$a,\ 2a,\ 3a,\ 4a,\ 5a,\ \ldots.\ (b-1)\,a$$

durch die andere Zahl a, so erhält man lauter unter einander verschiedene Reste.

Gesetzt es liessen zwei dieser Grössen ma und na denselben Rest, so wäre

$$ma \equiv na \pmod{b},$$

also, da a und b relative Primzahlen sind, durch Division mit a nach dem vierten Satze im vorigen §.:

$$m \equiv n \pmod{b},$$

d. h. es musste

$$\frac{m-n}{b} = Intg$$

sein, was offenbar, sobald m und n verschieden sind, nicht möglich ist. — Denn m und n sind aus der Zahlenreihe

$$1,\ 2,\ 3,\ 4,\ \ldots\ldots\ b-1$$

beliebig herausgegriffene Zahlen und darum jede für sich kleiner als b; mithin ist es um so stärker ihre Differenz.

Da nun die Reste, deren Verschiedenheit wir so eben bewiesen haben, alle für sich kleiner als b sind, so werden sie, etwaige Verschiedenheiten der Reihenfolge abgerechnet, mit der Reihe der natürlichen Zahlen von 1 bis $b-1$, nämlich

$$1,\ 2,\ 3,\ 4,\ 5,\ \ldots\ b-2,\ b-1$$

übereinstimmen oder, wenn wir die kleinsten Reste nehmen, im Falle eines geraden b mit der Reihe der Zahlen:

$$1,\ 2,\ 3,\ +\ldots\frac{b-2}{2},\ -\frac{b}{2},\ -\frac{b-2}{2},\ \ldots\ldots -3,\ -2,\ -1$$

und im Falle eines ungeraden b mit der Reihe der Zahlen:

$$1,\ 2,\ 3,\ \ldots + \frac{b-1}{2},\ -\frac{b-1}{2},\ \ldots\ldots -3,\ -2,\ -1.$$

Beispiel. Die beiden relativen Primzahlen seien 17 und 21; dann kann man zu Folge der Sätze 1) und 2) im vorhergehenden Paragraphen die kleinsten Reste der verschiedenen Vielfachen von 21 in Bezug auf den Modul 17 in folgender Weise erhalten:

$$\begin{array}{lll}
1.21 \equiv +4 & & 9.21 \equiv -2+4 \equiv +2 \\
2.21 \equiv 4+4 \equiv +8 & & 10.21 \equiv +2+4 \equiv +6 \\
3.21 \equiv 8+4 \equiv -5 & & 11.21 \equiv +6+4 \equiv -7 \\
4.21 \equiv -5+4 \equiv -1 & (mod\ 17) & 12.21 \equiv -7+4 \equiv -3 \\
5.21 \equiv -1+4 \equiv +3 & & 13.21 \equiv -3+4 \equiv +1 \\
6.21 \equiv +3+4 \equiv +7 & & 14.21 \equiv +1+4 \equiv +5 \\
7.21 \equiv +7+4 \equiv -6 & & 15.21 \equiv +5+4 \equiv -8 \\
8.21 \equiv -6+4 \equiv -2 & & 16.21 \equiv -8+4 \equiv -4
\end{array}$$

Sie sind mithin für sich allein zusammengestellt:

$$+4,\ +8,\ -5,\ -1,\ +3,\ +7,\ -6,\ -2,\ +2,\ +6,\ -7,\ -3,\ +1,\ +5,\ -8,\ -4,$$

oder auch, wenn man nur positive Reste zulassen will:

$$4,\ 8,\ 12,\ 16,\ 3,\ 7,\ 11,\ 15,\ 2,\ 6,\ 10,\ 14,\ 1,\ 5,\ 9,\ 13.$$

Das Theorem nun, auf welchem die Theorie der unbestimmten Gleichungen des ersten Grades beruht, lautet also:

Wenn a und b relative Primzahlen zu einander sind, so ist es immer möglich, für x solche ganzzahlige Werthe zu finden, durch welche der Congruenz

$$ax \equiv \pm c \pmod b$$

Genüge geschieht.

Der Beweis fliesst unmittelbar aus dem vorhergehenden Satze. Da die Vielfachen

$$a,\ 2a,\ 3a,\ 4a,\ 5a,\ \ldots.\ (b-2)a,\ (b-1)a$$

alle Reste lassen, welche bei der Division mit dem Modul b irgend nur vorkommen können, nämlich, wenn vielleicht auch in anderer Ordnung, die sämmtlichen Zahlen von 1 bis $n-1$ (so dass nur der Rest 0 ausgenommen ist, welcher einem Aufgehen der Division entspricht), so muss nothwendig eines unter diesen Vielfachen sein, welches denselben Rest lässt, wie die gegebene Zahl $\pm c$. Sei dieses Vielfache ma, so hat man

$$ma \equiv \pm c \pmod b$$

und es ist mithin die Existenz eines ganzzahligen Werthes m von x dargethan, welcher der vorgelegten Congruenz Genüge leistet. Wenn aber ein Werth gefunden ist, so sind damit unzählig viele solche Zahlen bestimmt, welche ihr gleichfalls genügen, nämlich alle solche Werthe von x, welche jenem Werthe nach dem Modul b congruent sind, und mithin kommt man schliesslich auf die Congruenz

$$x \equiv m \pmod b,$$

welche der gegebenen vollkommen gleich gilt.

Um dieses zu beweisen ist zweierlei darzuthun, einmal, dass alle Zahlen x, welche dieser Congruenz genügen, der gegebenen gleichfalls genügen. Dies erhellt unmittelbar. Denn wenn man sie mit a multiplizirt, so folgt nach dem zweiten Satze des vorigen Paragraphen:

$$ax \equiv am \pmod b,$$

also jedes x, welches ihr Genüge thut, macht den Ausdruck ax congruent mit am und, da am congruent mit $\pm c$ ist, auch congruent mit $\pm c$, d. h. es erfüllt die gegebene Congruenz. Weiter ist darzuthun, dass der Congruenz

$$ax \equiv \pm c \pmod b$$

keine Zahlen genügen können, die nicht auch die Congruenz

$$x \equiv m \pmod{b}$$

erfüllen. Nehmen wir also irgend eine Zahl x', die der gegebenen Congruenz genügt, so dass $ax' \equiv \pm c$ wird, dann folgt, durch Vergleichung mit der Congruenz $am \equiv \pm c$, die neue $ax' \equiv am \pmod{b}$ und diese reducirt sich durch Division mit a, welche statthaft ist, da a und b relative Primzahlen, auf $x' \equiv m \pmod{b}$ und das ist ja gerade die Congruenz, welche wir haben wollten. Also jeder Werth, der der Congruenz $ax \equiv \pm c \pmod{b}$ genügt, genügt auch der Congruenz $x \equiv m \pmod{b}$, und umgekehrt jeder Werth, welcher der zweiten Congruenz genügt, genügt auch der ersten. Hiernach ist die Congruenz

$$x \equiv m \pmod{b}$$

die Lösung der gegebenen Congruenz und zwar die einzige, die möglich ist.

Die Congruenz $ax \equiv \pm c$ ist offenbar nur ein abgekürzter Ausdruck der unbestimmten Gleichung ersten Grades mit zwei Unbekannten, nämlich:

$$ax - by = \pm c$$

und mithin ist die Auflösung einer solchen Gleichung auf die Auflösung der genannten Congruenz zurückführbar. In der That, wenn die Zahl m bestimmt ist, so stehen alle Zahlen, welche x mit m congruent machen, unter der Zahlform $x = m + Nb$, wo N irgend eine beliebige, positive oder negative, ganze Zahl bezeichnet. Setzen wir diesen Werth in unsere unbestimmte Gleichung ein, so bekommen wir $y = \frac{am \mp c}{b} + aN$, und es ist hier $\frac{am \mp c}{b}$ wegen der Congruenz $am \equiv \pm c$ eine ganze Zahl. Also genügt unserer Gleichung folgendes System von Werthen für x und y:

$$x = m + bN, \; y = \frac{am \mp c}{b} + aN.$$

Es sei z. B. die Gleichung

$$21x - 17y = -27$$

aufzulösen: so ist diese identisch mit der Congruenz

$$21x \equiv -27 \pmod{17}.$$

Da -27 den kleinsten Rest $+7$ lässt, so ergiebt ein Einblick in unsere obige Tabelle für den Modul 17 sogleich

$$6.21 \equiv -27 \ (mod\, 17),$$

also $m = 6$ und nun findet man für x und y leicht folgende Zahlformen:

$$x = 17N + 6, \ y = 21N + 9.$$

Was die Gleichung

$$ax + by = \pm c$$

betrifft, so führt sich diese gleichfalls sehr einfach auf die Auflösung der Congruenz $ax \equiv c \ (mod\, b)$ zurück, denn offenbar wird sie durch das System der Werthe

$$x = m + Nb, \ y = -\frac{am \mp c}{b} - aN$$

befriedigt und bedarf daher keiner besonderen Discussion. Betrachten wir z. B. der Gleichung

$$21x + 17y = -87,$$

so genügt die Congruenz

$$21x \equiv -87 \ (mod\, 17),$$

da der kleinste Rest von -87 die Zahl -2 ist, zu Folge der auf den Modul 17 bezüglichen Tabelle, der Werth $x = 8$ und man hat $m = 8$,

$$x = 8 + 17N, \ y = -15 - 21N.$$

Betrachten wir noch die Gleichung

$$21x + 17y = 87,$$

so bekommt man als einen speciellen Werth des x, welcher der Congruenz

$$21x \equiv 87 \ (mod\, 17)$$

Genüge leistet, $m = 9$ und mithin

$$x = 9 + 17N, \ y = -6 - 21N,$$

wo N wieder jede mögliche positive oder negative Zahl sein kann.

Fassen wir alles Vorhergehende zusammen, so erhellt, dass man die allgemeine Gleichung ersten Grades

$$ax \mp by = \pm c,$$

in der a und b positive ganze Zahlen bezeichnen, welche keinen gemeinschaftlichen Theiler besitzen, unter allen Umständen auflösen kann, und zwar führt sich ihre Auflösung auf die Auflösung der Congruenz

$$ax \equiv \pm c \ (mod\, b)$$

zurück. Diese letztere beruht nach dem Vorhergehenden auf der Ermittelung eines solchen Vielfachen von a, welches der Zahl $\pm c$ oder deren kleinstem Reste nach dem Modul b congruent ist. Diese Ermittelung ist immer einfach, denn sie setzt blos die Betrachtung einer beschränkten Anzahl von Vielfachen der a voraus. Wir wissen zunächst, dass diese Anzahl $= b-1$ ist. Aber sie kann um die Hälfte erniedrigt und mithin die Rechnung im entsprechenden Masse abgekürzt werden, wenn man den Satz benutzt, dass die im gleichen Abstande vom Ende befindlichen kleinsten Reste einander bis aufs Vorzeichen gleich sind. Um dieses zu erweisen, betrachte man ein beliebiges Paar im gleichen Abstande vom Ende befindlichen Vielfachen der Zahl a, etwa

$$ma \text{ und } (b-m)a,$$

und nehme an, dass ma den kleinsten Rest μ lasse. Dann ist

$$ma \equiv \mu \ (mod\, b),$$

und zieht man diese Congruenz von der folgenden,

$$ab \equiv 0 \ (mod\, b),$$

welche selbstverständlich besteht, ab, so ergiebt sich die Congruenz

$$(b-m)a \equiv -\mu \ (mod\, b),$$

in welcher der Satz liegt. In der That findet er sich auch durch die Betrachtung der obigen Tabelle für den Modul 17 bestätigt.

Trotz dieser Erleichterung ist aber, wenn a und b einigermassen gross sind, die Rechnung von ermüdender Weitschweifigkeit, und es ist daher gut, sich mit einer anderen Methode der Auflösung vertraut zu machen, welche die Zahlenrechnungen abkürzt. Diese Methode rührt von dem berühmten Lagrange her und beruht auf der Theorie der Kettenbrüche, über welche wir daher im nächsten Paragraphen das Nöthige beibringen wollen.

§. 6.

Von den Kettenbrüchen.

Unter einem Kettenbruche versteht man einen solchen Bruch, dessen Zähler eine ganze Zahl und dessen Nenner eine Summe ist, deren Ele-

mente wieder eine ganze Zahl und ein Bruch von derselben Beschaffenheit sind. Die allgemeine Form eines Kettenbruches ist daher

$$\cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ldots}}}$$

In dieser Allgemeinheit indessen brauchen wir die Betrachtung für die Bedürfnisse unserer Wissenschaft nicht aufzunehmen; denn in den Anwendungen kommen nur solche Kettenbrüche vor, deren Zähler sämmtlich der Einheit gleich und deren Nenner positive ganze Zahlen sind; ihre allgemeine Form ist:

$$\cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

und wir wollen hier die Nenner $a_1, a_2, a_3, \ldots$ mit dem Namen von Partialnennern oder Partialquotienten belegen.

Ein derartiger Kettenbruch kann mit der grössten Leichtigkeit aus jedem gemeinen Bruche hergestellt werden, und zwar werden seine Partialnenner durch dasselbe Verfahren geliefert, welches angewandt wird bei der Untersuchung, ob vielleicht der Zähler und Nenner des gegebenen Bruches einen gemeinschaftlichen Theiler besitzen.

Sei $\frac{A}{B}$ ein in den kleinsten Zahlen ausgedrückter ächter Bruch: dann kann man vermittelst des gewöhnlichen Divisionsverfahrens sich nach und nach folgende Gleichungen bilden:

$$\frac{B}{A} = a_1 + \frac{r_1}{A},\quad B = Aa_1 + r_1,$$

$$\frac{A}{r_1} = a_2 + \frac{r_2}{r_1},\quad A = r_1 a_2 + r_2,$$

$$\frac{r_1}{r_2} = a_3 + \frac{r_3}{r_2},\quad r_1 = r_2 a_3 + r_3,$$

$$\frac{r_2}{r_3} = a_4 + \frac{r_4}{r_3},\quad r_1 = r_3 a_4 + r_4,$$

$$\cdots\cdots$$

$$\cdots\cdots$$

$$\frac{r_{n-3}}{r_{n-2}} = a_{n-1} + \frac{r_{n-1}}{r_{n-2}},\quad r_{n-3} = r_{n-2} a_{n-1} + r_{n-1},$$

$$\frac{r_{n-2}}{r_{n-1}} = a_n + \frac{r_n}{r_{n-1}},\quad r_{n-2} = r_{n-1} a_n + r_n.$$

Aus der Betrachtung dieser Gleichungen ist klar, dass die r sich mehr und mehr verkleinern und dass mithin, da sie immer ganze Zahlen bleiben, eines nothwendig irgend einmal den Werth 1 erreichen muss; der Werth des nachfolgenden r wird dann 0, weil 1 in jede Zahl aufgeht und die Rechnung bricht demgemäss ab, und zwar sind die beiden Schlussreste

$$r_{s-1},\ r_s = 0.$$

Man könnte gegen diese Schlussweise die einzige Einwendung machen, dass vielleicht einmal der Rest 0 kommen könnte, ohne dass der vorhergehende Rest den Werth 1 habe. Aber es lässt sich dann leicht zeigen, dass dieser Rest dann ein gemeinschaftlicher Theiler von A und B sein müsste, im Widerspruche zu der Voraussetzung, nach der $\frac{A}{B}$ ein in den kleinsten Zahlen ausgedrückter Bruch ist. Sei z. B. $r_4 = 0$, so müsste r_3 in r_2 aufgehen, und darum wegen der Gleichung

$$r_1 = r_2 a_3 + r_3,$$

in deren rechte Seite es ohne Rest dividirbar wäre, auch in r_1. Nun ginge r_3 gleichzeitig in r_1 und r_2 auf, also wegen der Gleichung

$$A = r_1 a_2 + r_2$$

auch in A; endlich ginge es jetzt zu gleicher Zeit in A und r_1 auf, darum wegen der Gleichung

$$B = A a_1 + r_1$$

auch in B; mithin wäre es ein gemeinschaftlicher Theiler von A und B.

Giebt man jetzt dem Bruche $\frac{A}{B}$ die Form $\frac{1}{\frac{B}{A}}$, so folgt mit Rücksicht auf das eben aufgestellte Formelsystem

$$\frac{A}{B} = \cfrac{1}{a_1 + \cfrac{r_1}{A}} = \cfrac{1}{a_1 + \cfrac{1}{\cfrac{A}{r_1}}}$$

$$= \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{r_2}{r_1}}} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cfrac{r_1}{r_2}}}}$$

$$= \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{r_3}{r_2}}}} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cfrac{r_2}{r_3}}}}}$$

. . . .

. . . .,

$$= \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ldots\ldots,}}}}$$

$$\ldots\ldots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}.$$

Es ist umgekehrt eben so leicht einen Kettenbruch in einen gemeinen Bruch zu verwandeln. So z. B. ist in Uebereinstimmung mit der unmittelbar vorhergehenden Entwickelung

$$\cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{r_3}{r_2}}}} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{r_2}{r_1}}} = \cfrac{1}{a_1 + \cfrac{r_1}{A}} = \frac{A}{B}.$$

Das allgemeine Verfahren erhellt auch aus den obigen Gleichungen für

$$\frac{B}{A}, \frac{r_1}{A}, \frac{r_2}{r_1}, \frac{r_3}{r_2}, \ldots\ldots \frac{r_{n-2}}{r_{n-1}}.$$

Denn ausser dem Quotienten a sind noch die beiden Reste $r_{n-1} = A$, $r_n = 0$ bekannt; mithin folgt aus der letzten dieser Gleichungen der Werth r_{n-2}, darauf, indem man diesen Werth in die vorhergehende Gleichung einsetzt, der Werth von r_{n-3}. Diesen Werth setzt man wieder in die drittletzte Gleichung ein und bekommt so r_{n-4} und indem man so weiter fortgeht, gelangt man aufsteigend zu den Werthen von A und B.

Die Kettenbrüche

$$\frac{1}{a_1}, \quad \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \quad \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}}, \quad \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}}, \ldots\ldots$$

welche, je nach der Anzahl der in ihnen vorkommenden Partialnenner, 1, 2, 3, 4, ... gliedrige heissen sollen und welche aus der Entwickelung des Bruches $\frac{A}{B}$ hervorgehen durch successive Vernachlässigung der Grössen

$$\frac{r_1}{A}, \frac{r_2}{r_1}, \frac{r_3}{r_2}, \frac{r_4}{r_3} \ldots\ldots,$$

heissen respective der erste, zweite, dritte, vierte, ... Näherungsbruch zu dem Werthe des Kettenbruches, weil, wie sich später erge-

ben wird, man dem Werthe des Kettenbruches um so näher kommt, je mehr Glieder man zusammennimmt. Vorläufig kann man gleich bemerken, dass der erste Näherungsbruch grösser ist, als der gegebene Bruch $\frac{A}{B}$; denn es fehlt seinem Nenner a_1 eine positive Grösse, welche hinzutreten müsste, damit er dem Bruche $\frac{A}{B}$ gleich würde, also ist a_1 zu klein und mithin $\frac{1}{a_1}$ zu gross. Der zweite Näherungsbruch hingegen ist kleiner als $\frac{A}{B}$; denn es fehlt dem Nenner a_2 eine positive Quantität, welche hinzutreten müsste, damit er gleich $\frac{A}{B}$ würde; also ist für diesen Zweck a_2 zu klein, $\frac{1}{a_2}$ zu gross und mithin auch $a_1 + \frac{1}{a_2}$, also

$$\frac{1}{a_1 + \frac{1}{a_2}} = \frac{1}{a_1} + \frac{1}{a_2}$$

zu klein. Der dritte Näherungsbruch ist wiederum grösser als der gegebene Bruch $\frac{A}{B}$. Denn damit er gleich diesem Bruche ausfiele, müsste zu a_3 etwas hinzutreten; also ist a_3 zu klein, $\frac{1}{a_3}$ zu gross und mithin auch $a_2 + \frac{1}{a_3}$, also

$$\frac{1}{a_2 + \frac{1}{a_3}} = \frac{1}{a_2} + \frac{1}{a_3}$$

zu klein und mithin auch

$$a_1 + \frac{1}{a_2} + \frac{1}{a_3};$$

hieraus folgt endlich

$$\frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} = \frac{1}{a_1 +} \frac{1}{a_2} + \frac{1}{a_3}$$

zu gross. Diese Schlussweise lässt sich beliebig weit fortsetzen und es erhellt daher das Theorem:

Die Näherungsbrüche zu dem Werthe eines Kettenbruches sind an den ungeraden Stellen zu gross, an den geraden Stellen zu klein. Der wahre Werth eines Kettenbruches ist daher zwischen zwei aufeinander folgenden Näherungsbrüchen enthalten.

Als Rechnungsbeispiel möge der Bruch $\frac{279}{911}$ dienen.

```
279|911|3
    837
     74|279|3
        222
         57|74|1
            57
            17|57|3
               51
                6|17|2
                  12
                   5|6|1
                     5
                     1|5|5
```

, also
$$\frac{279}{911} = \cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{5}}}}}}}$$

Die Näherungsbrüche sind

$$1)\ \frac{1}{3} = \frac{1}{3},\quad 2)\ \cfrac{1}{3+\cfrac{1}{3}} = \frac{3}{10},\quad 3)\ \cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{1}}} = \frac{4}{13},$$

$$4)\ \cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3}}}} = \frac{15}{49},\quad 5)\ \cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2}}}}} = \frac{34}{111},$$

$$6)\ \cfrac{1}{3+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{1}}}}}} = \frac{49}{160}$$

und der Werth des gemeinen Bruches $\frac{279}{911}$ daher enthalten zwischen $\frac{1}{3}$ und $\frac{3}{10}$, mithin da

$$\frac{1}{3} - \frac{3}{10} = \frac{1}{3.10}$$

der Fehler geringer als $\frac{1}{30}$, wenn man einen dieser Brüche für $\frac{279}{911}$ setzt; ebenso ist $\frac{279}{911}$ enthalten zwischen $\frac{3}{10}$ und $\frac{4}{13}$, also, da

$$\frac{4}{13}-\frac{3}{10}=\frac{1}{10.13}$$

der Fehler noch nicht $\frac{1}{130}$, wenn man einen dieser beiden Näherungsbrüche an Stelle des gegebenen Bruches setzt. Ferner ist der gegebene Bruch enthalten zwischen den Näherungsbrüchen $\frac{4}{13}$ und $\frac{15}{49}$, also, da

$$\frac{4}{13}-\frac{15}{49}=\frac{1}{13.49}$$

ist, der Fehler geringer als $\frac{1}{637}$, wenn man einen dieser beiden letzten Brüche an Stelle des gegebenen Bruches substituirt. Indem man diese Rechnung fortsetzt, gewinnt man für den vorliegenden Fall empirisch die Ueberzeugung, dass die Näherungsbrüche in der That immer genauer an den Werth des Kettenbruches heranstreifen, je mehr Glieder desselben genommen werden, sowie, dass der Unterschied zweier aufeinanderfolgenden Näherungsbrüche (dieselben als auf die gemeine Bruchform reducirt vorausgesetzt) gleich ist einem Bruche, dessen Zähler 1 und dessen Nenner das Produkt der Nenner von den beiden betrachteten Näherungsbrüchen ist.

Bezeichnen wir jetzt, um das Gesetz für die Bildung der Näherungsbrüche aufzudecken, dieselben der Reihe nach mit

$$\frac{Z_1}{N_1},\ \frac{Z_2}{N_2},\ \frac{Z_3}{N_3},\ \frac{Z_4}{N_4},\ldots\ldots$$

so folgt durch successive Entwickelung

$$\frac{Z_1}{N_1}=\frac{1}{a_1},$$

$$\frac{Z_2}{N_2}=\frac{1}{a_1+\frac{1}{a_2}}=\frac{a_2 . 1}{a_2 . a_1+1}=\frac{a_2 Z_1}{a_2 N_1+1},$$

$$\frac{Z_3}{N_3}=\frac{\left(a_2+\frac{1}{a_3}\right)Z_1}{\left(a_2+\frac{1}{a_3}\right)N_1+1}=\frac{a_3 . a_2 Z_1+Z_1}{a_3(a_1 N_1+1)+N_1}=\frac{a_3 . Z_2+Z_1}{a_3 . N_2+N_1},$$

$$\frac{Z_4}{N_4}=\frac{\left(a_3+\frac{1}{a_4}\right)Z_2+Z_1}{\left(a_3+\frac{1}{a_4}\right)N_2+N_1}=\frac{a_4(a_3 Z_2+Z_1)+Z_2}{a_4(a_3 N_2+N_1)+N_2}=\frac{a_4 . Z_3+Z_2}{a_4 . N_3+N_2},$$

. . . . . .

. . . . . .

Die Betrachtung dieser Resultate ergiebt sogleich die Recursionsformel:

$$\frac{Z_m}{N_m} = \frac{a_m \cdot Z_{m-1} + Z_{m-2}}{a_m \cdot N_{m-1} + N_{m-2}},$$

die man, wenn man will, sich durch eine leichte Induction beweisen kann. Hiernach bekommt man folgendes Bildungsgesetz:

Um den Zähler irgend eines Näherungsbruches zu erhalten, multiplicire man den bezüglichen Partialquotienten in den Zähler des unmittelbar vorhergehenden Näherungsbruches und addire zu dem Produkte den Zähler des zweitvorhergehenden Näherungsbruches. Der Nenner wird durch eine analoge Rechnung mit den Nennern der beiden vorhergehenden Näherungsbrüche erhalten.

Dies Verfahren ist blos auf den ersten und zweiten Näherungsbruch nicht anwendbar; doch kann man es durch einen Kunstgriff wenigstens noch auf den zweiten ausdehnen, nämlich wenn man $\frac{0}{1}$ als den 0ten Näherungsbruch ansieht. Das Technische des Verfahrens möge das nachfolgende Beispiel erläutern, zu welchem der oben aus dem gemeinen Bruche $\frac{279}{911}$ hergeleitete Kettenbruch benutzt ist.

	3	3	1	3	2	1	5
$\frac{0}{1}$	$\frac{1}{3}$	$\frac{3}{10}$	$\frac{4}{13}$	$\frac{15}{49}$.	$\frac{34}{111}$	$\frac{49}{160}$	$\frac{279}{911}$

Die Bildung der Näherungsbrüche erhellt näher aus den Gleichungen

$$\frac{3}{10} = \frac{3.1+0}{3.3+1}, \quad \frac{4}{13} = \frac{1.3+1}{1.10+3}, \quad \frac{15}{49} = \frac{3.4+3}{3.13+10} \text{ u. s. w.}$$

Bilden wir uns jetzt die Differenz irgend zweier aufeinanderfolgenden Näherungsbrüche, so erhalten wir zunächst

$$\frac{Z_m}{N_m} - \frac{Z_{m-1}}{N_{m-1}} = \frac{Z_m N_{m-1} - Z_{m-1} N_m}{N_m N_{m-1}}.$$

Nun ist aber auch auf der andern Seite zu Folge des Werthes von $\frac{Z_m}{N_m}$ dieselbe Differenz

$$= \frac{a_m Z_{m-1} + Z_{m-2}}{a_m N_{m-1} + N_{m-2}} - \frac{Z_{m-1}}{N_{m-1}}$$

$$= \frac{Z_{m-2} N_{m-1} - Z_{m-1} N_{m-2}}{(a_m N_{m-1} + N_{m-2}) N_{m-1}}$$

$$= \frac{-(Z_{m-1} N_{m-2} - Z_{m-2} N_{m-1})}{N_m \cdot N_{m-1}}.$$

Setzen wir beide Werthe einander gleich, so folgt die Relation

$$Z_m N_{m-1} - Z_{m-1} N_m = -(Z_{m-1} N_{m-2} - Z_{m-2} N_{m-1}),$$

woher durch Einsetzung von $m-1$, $m-2$, $m-3$, ... $m-(m-3)$ an die Stelle von m folgendes System von Formeln fliesst:

$$Z_{m-1} N_{m-2} - Z_{m-2} N_{m-1} = -(Z_{m-2} N_{m-3} - Z_{m-3} N_{m-2}),$$

$$Z_{m-2} N_{m-3} - Z_{m-3} N_{m-2} = -(Z_{m-3} N_{m-4} - Z_{m-4} N_{m-3}),$$

. . . .

$$Z_3 N_2 - Z_2 N_3 = -(Z_2 N_1 - Z_1 N_2)$$

und setzen wir hier von der untersten aufsteigend jede Formel in die nächst höhere ein, so ergiebt sich schliesslich, da wir im Ganzen $(m-2)$ Gleichungen haben

$$Z_m N_{m-1} - Z_{m-1} N_m = (-1)^{m-2}(Z_2 N_1 - Z_1 N_2).$$

Nun ist

$$\frac{Z_2}{N_2} - \frac{Z_1}{N_1} = \frac{a_2}{a_2 a_1 + 1} - \frac{1}{a_1} = \frac{-1}{a_1(a_2 a_1 + 1)} = \frac{Z_2 N_1 - Z_1 N_2}{a_1(a_2 a_1 + 1)},$$

also die auf der rechten Seite der vorhergehenden Gleichung in Klammern gesetzte Grösse gleich -1 und wir erhalten daher die wichtige Relation

$$Z_m N_{m-1} - Z_{m-1} N_m = (-1)^{m-1},$$

woher noch sogleich die andere

$$\frac{Z_m}{N_m} - \frac{Z_{m-1}}{N_{m-1}} = \frac{(-1)^{m-1}}{N_m N_{m-1}}$$

folgt. Wir haben dem zu Folge das Theorem:

Der Unterschied zweier Näherungsbrüche ist gleich einem Bruche, dessen Nenner das Produkt aus beiden Nennern und dessen Zähler gleich ± 1 ist, nämlich gleich $+1$, wenn der Minuendus ein Näherungsbruch mit ungerader Gliederzahl, und -1, wenn der Minuendus ein Näherungsbruch mit gerader Gliederzahl ist.

Aus diesem Theoreme ergeben sich sogleich mehrere bemerkenswerthe Folgerungen:

Die Zähler und Nenner eines Näherungsbruches sind relative Primzahlen und es existirt kein Bruch in kleineren Zahlen, welcher dem Werthe des Kettenbruches näher komme.

Das Erste ergiebt sich zu Folge der Gleichung

$$Z_m N_{m-1} - Z_{m-1} N_m = (-1)^{m-1};$$

denn wenn Z_m und N_m einen gemeinschaftlichen Faktor hätten, so müsste derselbe auch die rechte Seite der Gleichung, d. h. die Einheit theilen; mithin kann er nur der Einheit selber gleich sein. Das Zweite folgt apagogisch. Existirte ein Bruch in kleineren Zahlen als $\frac{Z_m}{N_m}$, etwa $\frac{x}{y}$, welcher dem Werthe des Kettenbruches näher käme, so wären $\frac{x}{y}$ und $\frac{Z_{m-1}}{N_{m-1}}$ zwei nähere Grenzzahlen für diesen Werth, als $\frac{Z_m}{N_m}$ und $\frac{Z_{m-1}}{N_{m-1}}$, mithin folgte, ohne Rücksicht auf das Vorzeichen und blos in Rücksicht der absoluten Werthe:

$$\frac{x}{y}-\frac{Z_{m-1}}{N_{m-1}}<\frac{Z_m}{N_m}-\frac{Z_{m-1}}{N_{m-1}},$$

also

$$xN_{m-1}-yZ_{m-1}<(Z_mN_{m-1}-Z_{m-1}N_m)\frac{y}{N_m}.$$

Der erste Faktor auf der rechten Seite hat den Werth 1, der zweite Faktor ist, da nach der Annahme $y<N_m$ ist, ein ächter Bruch und wir bekommen daher

$$xN_{m-1}-yZ_{m-1}<1,$$

welches ein Widersinn ist, da die Differenz zwischen zwei ganzzahligen Ausdrücken niemals gebrochen sein kann.

Indem daher die Näherungsbrüche bei den kleinsten Zahlen die grösste Näherung geben, haben sie ein ganz vorzügliches Recht auf den Namen, den sie führen.

Wenn der gegebene Bruch, der uns einen Kettenbruch liefert, unächt ist, so hat letzterer die Form

$$\frac{A}{B}=a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\ldots}}}$$

und es fragt sich, wie sich für diesen Fall die Näherungsbrüche ergeben. Der nächst liegende Gedanke ist hier wohl sich die Näherungsbrüche zu dem umgekehrten Bruche

$$\frac{B}{A}=\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ldots}}}$$

zu suchen und dieselben umzukehren. Aber haben diese umgekehrten Näherungsbrüche auch dieselben Eigenschaften, wie die früheren? Diese Frage beantwortet sich, indem man mit $\frac{N_m}{Z_m}$ und $\frac{N_{m-1}}{Z_{m-1}}$ zwei aufeinanderfolgende Näherungsbrüche des ächten Bruches $\frac{A}{B}$ bezeichnet, durch die Betrachtung der Gleichung

$$N_m Z_{m-1} - N_{m-1} Z_m = (-1)^{m-1},$$

aus welcher die Differenz der unächten Näherungsbrüche

$$\frac{Z_{m-1}}{N_{m-1}} - \frac{Z_m}{N_{m-1}} = \frac{(-1)^{m-1}}{N_m N_{m-1}}$$

folgt; die umgekehrten Näherungsbrüche haben demgemäss ganz die Eigenschaften der ursprünglichen und sind nur dadurch unterschieden, dass sie, was ohnehin selbstverständlich ist, an den ungeraden Stellen zu klein und an den geraden zu gross sind.

Praktisch ist es wohl zweckmässig sich in einem solchen Falle unmittelbar $\frac{1}{0}$ als den 0ten und $\frac{a_1}{1}$ als den ersten Näherungsbruch hinzuschreiben und die übrigen nach dem oben aufgestellten Bildungsgesetz sich successive zu berechnen, wie es an folgendem Beispiele gezeigt werden soll.

```
6654|29657|4,
     26616
      3041|6654|2
           6082
            572|3041|5
                2860
                 181|572|3
                     543
                      29|181|6
                         174
                           7|29|4
                             28
                              1|7|7
```

also $\frac{29657}{6654} = 4 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{4 + \cfrac{1}{7}}}}}}$

	4	2	5	3	6	4	7
$\frac{1}{0}$	$\frac{4}{1}$	$\frac{9}{2}$	$\frac{49}{11}$	$\frac{156}{35}$	$\frac{985}{221}$	$\frac{4096}{916}$	$\frac{29657}{6554}$

Zur Vervollständigung der Theorie ist noch eine Betrachtung wesentlich. Wir haben im Vorhergehenden die stillschweigende Voraussetzung gemacht, dass ein endlicher Werth des Kettenbruches, mit dem die Grösse der Näherungswerthe verglichen werden könne, existire — und diese Veraussetzung war allerdings insofern berechtigt, als wir nur Kettenbrüche mit endlicher geschlossener Gliederzahl in den Kreis unserer Untersuchung zogen, nämlich solche, welche genau einer gegebenen Zahl in gewöhnlicher Bruchform gleich waren. Die Untersuchung ist mithin nahe gelegt, ob ein endlicher und bestimmter Werth eines Kettenbruches nicht auch bei unendlicher Gliederzahl existiren könne, und wenn es uns gelingen sollte, den Nachweis für seine Existenz zu liefern, so wären wir vollständig berechtigt, nicht blos die Sätze über die formale Bildung der Näherungsbrüche, sondern auch die Sätze, die eine Werthvergleichung der Näherungsbrüche mit dem Werthe des Kettenbruches enthalten, auf diesen Fall auszudehnen.

Bei den engen Grenzen, innerhalb deren unsere Discussion sich bewegt, da wir blos ganze und positive Partialnenner zulassen, ist die Entscheidung unschwer zu treffen.

Aus dem formalen Bildungsgesetze ist evident, dass die Nenner der Näherungsbrüche mit dem Index wachsen und zwar nehmen sie in einem stärkeren Verhältnisse zu, als die Reihe der natürlichen Zahlen zunimmt. Sie werden mithin, wenn der Index m über jede Grenze hinaus zunimmt, gleichfalls unendlich gross und das Nämliche gilt um so stärker von dem Produkte zweier solcher benachbarten Nenner

Nun ist der Unterschied zweier benachbarten Näherungsbrüche

$$\frac{Z_m}{N_m} - \frac{Z_{m-1}}{N_{m-1}} = \frac{(-1)^{m-1}}{N_m N_{m-1}};$$

er muss mithin bei unendlicher Gliederzahl verschwinden; denn der Werth eines Bruches nimmt über jede Grenze hinaus ab, wenn der Nenner über jede Grenze hinaus wächst.

Hiernach ist klar, dass man, jemehr Glieder des Kettenbruches man nimmt, man sich um so stärker einer festen unveränderlichen Grenze nähert, welcher die Näherungsbrüche mit wachsendem Index entgegenconvergiren, und diese feste Grenze ist das, was wir den Werth des Kettenbruches nennen.

Es ist jetzt noch der Nachweis übrig, dass diese feste unveränderliche Grenze eine endliche, bestimmte Grösse ist und nicht etwa entweder ins Unendliche wächst oder ins Unendliche abnimmt. Zu dem Zwecke bilden wir uns nach der Reihe die Gleichungen

$$\frac{Z_1}{N_1}-\frac{Z_2}{N_2}=\frac{1}{N_1 . N_2},$$

$$\frac{Z_2}{N_2}-\frac{Z_3}{N_3}=-\frac{1}{N_2\,N_3},$$

$$\frac{Z_3}{N_3}-\frac{Z_4}{N_4}=+\frac{1}{N_3\,N_4},$$

$$\frac{Z_4}{N_4}-\frac{Z_5}{N_5}=-\frac{1}{N_4\,N_5}$$

$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

$$\frac{Z_{m-1}}{N_{m-1}}-\frac{Z_m}{N_m}=(-1)^m\frac{1}{N_{m-1}\,N_m}$$

und addiren dieselben alle zusammen. Dadurch ergiebt sich, da sich links alle Glieder bis auf das erste und letzte heben,

$$\frac{Z_1}{N_1}-\frac{Z_m}{N_m}=\frac{1}{N_1N_2}-\frac{1}{N_2N_3}+\frac{1}{N_3N_4}-\frac{1}{N_4N_5}+\cdots\cdots$$
$$+(-1)^{m-1}\frac{1}{N_{m-2}\,N_{m-1}}+(-1)^m\frac{1}{N_{m-1}\,N_m}.$$

Die rechte Seite dieser Gleichung ist eine Reihe, deren Glieder abwechselnd positiv und negativ sind und, wenn man den Index m ins Unendliche hinein wachsen lässt, zuletzt über jede Grenze hinaus abnehmen. Sie ist daher nach einem bekannten Theoreme der Analysis eine convergente Reihe, d. h. sie hat eine endliche und bestimmte Grösse zur Summe. Uebrigens ist es, auch wenn man dieses Theorem nicht voraussetzen will, leicht den Beweis zu führen, dass die Summe der Reihe zwischen zwei endlichen Quantitäten enthalten ist. Bringt man sie nämlich, indem man zuerst das erste und zweite, darauf das dritte und vierte Glied, das fünfte und sechste u. s. w. zusammennimmt, auf die Form

$$\frac{N_3-N_1}{N_1N_2N_3}+\frac{N_5-N_3}{N_3N_4N_5}+\frac{N_7-N_5}{N_5N_6N_7}+\cdots\cdots\cdots,$$

so erhellt sogleich, dass jedes Glied positiv ist, da die N mit dem Wachsen der Index immer zunehmen und dem zu Folge die Differenzen

$$N_3 - N_1,\ N_5 - N_3,\ N_7 - N_5, \ldots.$$

positiv ausfallen. Daher ist die Summe sämmtlicher Glieder mit Nothwendigkeit grösser als das erste Glied, wie gross der Index m auch genommen werden möge. Man kann aber auch unserer Reihe folgende Form geben:

$$\frac{1}{N_1 N_2} - \frac{N_4 - N_2}{N_2 N_3 N_4} - \frac{N_6 - N_4}{N_4 N_5 N_6} - \frac{N_8 - N_6}{N_6 N_7 N_8} - \ldots\ldots$$

und da hier alle Glieder bis aufs erste negativ sind, so ist die Summe sämmtlicher Glieder, wie gross m auch sein möge, kleiner als das erste positive Glied $\frac{1}{N_1 N_2}$. Hiernach ist für jeden beliebig grossen Werth von m die Summe der Reihe zwischen $\frac{1}{N_1 N_2}$ und $\frac{N_3 - N_1}{N_1 N_2 N_3}$ enthalten und liegt also auch noch in dem Falle selber, dass m ins Unendliche hinein wachse, zwischen den genannten Quantitäten, die für endliche a_1, a_2, a_3, wie wir sie voraussetzen, immer endlich und bestimmt ausfallen: mithin muss auch die dazwischen liegende Grösse, die Summe der unendlichen Reihe, eine endliche und bestimmte Quantität sein.

Wir haben jetzt bewiesen, dass der Ausdruck

$$\frac{Z_1}{N_1} - \frac{Z_m}{N_m},$$

auch wenn m ins Unendliche hinein wächst, einen endlichen und bestimmten Werth bekommt. Da nun der erste Theil desselben immer einen endlichen und bestimmten Werth hat, so ist dieses nicht anders möglich, als wenn dasselbe auch von dem zweiten Theile gilt und das wollten wir eben beweisen.

Hiermit hat es einen bestimmten Sinn gewonnen, wenn wir unendliche Kettenbrüche im Folgenden etwa den Operationen des Calculs unterziehen sollten; wir gehen damit im Grunde ebensowenig über die Rechnung mit endlichen bestimmten Grössen hinaus, wie es der Fall ist bei Kettenbrüchen mit geschlossener Gliederzahl.

Betrachten wir jetzt einen beliebigen Kettenbruch von n Gliedern:

und bilden die Reihe der Näherungsbrüche, so werden wir, bei einer genaueren Betrachtung des nachfolgenden Schemas, durch welches sie allmählig erhalten werden:

	a_1	a_2	a_3	a_4
$\frac{1}{0}$	$\frac{a_1}{1}$	$\frac{a_2 a_1 + 1}{a_2}$	$\frac{a_3 a_2 a_1 + a_3 + a_1}{a_3 a_2 + 1}$	$\frac{a_4 a_3 a_2 a_1 + a_4 a_3 + a_4 a_1 + a_2 a_1 + 1}{a_4 a_3 a_2 + a_4 + a_2}$

sogleich die Bemerkung machen, dass jeder Nenner aus dem Zähler des nächstvorhergehenden Näherungsbruches durch die einfache Erhöhung der Indices von a um 1 erhalten wird, und dies ist eine nothwendige Folge davon, dass der Zähler Z_{n-1} offenbar gerade so aus 1, a_1, a_2, a_3 .... a_{n-1} gebildet wird, wie der Nenner N_n aus 1, a_2, a_3, a_4, ... a_n. Zugleich werden sowohl die sämmtlichen Zähler, wie die sämmtlichen Nenner durch die Aufeinanderfolge der Partialquotienten, die zu ihrer Bildung verwandt werden, vollständig bestimmt und wir können daher

$$Z_n = f(a_1, a_2, a_3, \ldots a_n),$$
$$N_n = f(a_2, a_3, a_4, \ldots a_n)$$

oder kürzer, indem wir blos den ersten und letzten Index hinschreiben und die übrigen auslassen

$$Z_n = f(1, n),$$
$$N_n = f(2, n)$$

setzen. Um die Natur der Function f kennen zu lernen, genügt es, sich auf die Betrachtung der Zähler zu beschränken, da die Nenner vollkommen gleich gebildet werden.

Es ist hier nicht der Ort, um ausführlich auf ihre Discussion einzugehen und wir begnügen uns daher nur eine bemerkenswerthe Eigenschaft, die sie besitzt, hervorzuheben, nämlich dass die Ordnung der Elemente a umgekehrt werden kann, ohne dass sie irgendwie dadurch verändert werde. In der That wird der Satz durch die Betrachtung der speciellen Fälle

$$f(1, 2) = a_2 a_1 + 1 = a_1 a_2 + 1 = f(2, 1),$$
$$f(1, 3) = a_3 a_2 a_1 + a_3 + a_1 = a_1 a_2 a_3 + a_1 + a_3 = f(3, 1)$$

verificirt und um ihn allgemein zu beweisen, wollen wir darthun, dass, wenn er für irgend drei aufeinanderfolgende solcher Functionen gültig

ist, er auch die nächst höhere Geltung hat, oder in Zeichen, dass wenn man

$$f(1,\ n-3)=f(n-3,\ 1),$$
$$f(1,\ n-2)=f(n-2,\ 1),$$

und

$$f(1,\ n-1)=f(n-1,\ 1)$$

hat, daraus

$$f(1,\ n)=f(n,\ 1)$$

folgt.

Zu dem Zwecke bemerken wir, dass unsere Recursionsformel zur Berechnung der Zähler

$$Z_m = a_m Z_{m-1} + Z_{m-2}$$

zu Folge der eingeführten Bezeichnung übergeht in

$$f(1,\ m) = a_m f(1,\ m-1) + f(1,\ m-2)$$

und mithin ist

$$f(1,\ n) = a_n f(1,\ n-1) + f(1,\ n-2)$$

oder in Anwendung der Voraussetzung

$$= a_n f(n-1,\ 1) + f(n-2,\ 1).$$

Indem man hier nochmals die Recursionsformeln

$$f(n-1,\ 1) = a_1 f(n-1,\ 2) + f(n-1,\ 3),$$
$$f(n-2,\ 1) = a_1 f(n-1,\ 2) + f(n-2,\ 3)$$

substituirt, bekommen wir

$$f(1,n) = a_n a_1 f(n-1,\ 2) + a_n f(n-1,\ 3) + a_1 f(n-2, 2) + f(n-2, 3).$$

Nun ist zu Folge der Erklärung unserer Function die Natur ihrer Zusammensetzung blos von der Anzahl und der Ordnung der Elemente a abhängig; mithin, wenn die Formeln

$$f(1, n-3) = f(n-3,\ 1),\ f(1,\ n-2) = f(n-2, 1)$$

bestehen, so werden dieselben nicht aufhören zu gelten, wenn man die Indices 1 und $n-3$ oder 1 und $n-2$ zu gleicher Zeit entweder um dieselbe Grösse vermehrt oder verringert; denn dadurch wird möglicherweise der Zahlenwerth der Elemente $a_1,\ a_2,\ a_3, \ldots.,$ welche in die Formel hineingehen, geändert, aber keinesfalls weder die Anzahl, noch die Ordnung, in der sie zur Bildung der Function f verwandt werden. Wir erhalten also aus den vorstehenden Gleichungen

$$f(2,\ n-2) = f(n-2,\ 2);\ f(3, n-1) = f(n-1, 3);$$
$$f(2,\ n-1) = f(n-1,\ 2)$$

und wenn wir diese Gleichungen in die rechte Seite des Ausdruckes für $f(1, n)$ einsetzen, so resultirt

$$f(1, n) = a_n a_1 f(2, n-1) + a_n f(3, n-1) + a_1 f(2, n-2) + f(3, n-2)$$
$$= a_1[a_n f(2, n-1) + f(2, n-2)] + [a_n f(3, n-1) + f(3, n-2)]$$

Hier erkennt man sogleich, dass zu Folge der allgemeinen Recursionsformel die Ausdrücke in den eckigen Klammern respective den Ausdrücken

$$f(2, n),\ f(3, n)$$

gleich sind, und wenn man nun noch hinzunimmt, dass aus den Gleichungen

$$f(1, n-1) = f(n-1, 1),$$
$$f(2, n-1) = f(n-1, 2)$$

durch Erhöhung der Indices respective um eine Einheit die neuen Gleichungen

$$f(2, n) = f(n, 2),$$
$$f(3, n) = f(n, 3)$$

hervorgehen, so bekommt man an Stelle der letzten Gleichung für $f(1, n)$ die neue

$$f(1, n) = a_1 f(n, 2) + f(n, 3),$$

aus der durch eine abermalige Anwendung der allgemeinen Recursionsformel die Schlussgleichung

$$f(1, n) = f(n, 1)$$

hervorgeht.

Mithin, wenn der ausgesprochene Satz für die Zusammensetzung aus $n-3$, $n-2$, $n-1$ Elementen richtig ist, so ist er auch für die Zusammensetzung aus n Elementen gültig. Da er nun für die aus 1, 2, 3 Elementen sich bildenden Functionenformen thatsächlich Geltung hat, so ist er allgemein gültig.

Vergleichen wir jetzt die Werthe der beiden Kettenbrüche

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 \cdots\cdots \cdots + \cfrac{1}{a_n}}}}, \quad a_n + \cfrac{1}{a_{n-1} + \cfrac{1}{a_{n-2} + \cfrac{1}{a_{n-3} \cdots\cdots \cdots + \cfrac{1}{a_1}}}}$$

mit einander, so findet man auf die gewöhnliche Weise den Werth des ersten gleich $\frac{Z_n}{N_n}$ oder, wenn wir wieder unsere neue Bezeichnung anwen-

den, gleich $\frac{f(1,n)}{f(2,n)}$; der Werth des zweiten dagegen ist

$$\frac{f(n,1)}{f(n-1,1)} = \frac{f(1,n)}{f(1,n-1)} = \frac{Z_n}{Z_{n-1}}.$$

Dem zu Folge ergeben sich die Gleichungen:

$$\frac{Z_n}{N_n} = \frac{f(1,n)}{f(2,n)} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots\dots + \frac{1}{a_n}}}}$$

und

$$\frac{Z_n}{Z_{n-1}} = \frac{f(1,n)}{f(1,n-1)} = a_n + \frac{1}{a_{n-1} + \frac{1}{a_{n-2} + \frac{1}{a_{n-3} + \dots\dots + \frac{1}{a_1}}}}$$

Die Bedingungsgleichung dafür, dass beide Kettenbrüche einander gleich werden, ist

$$Z_{n-1} = N_n$$

oder

$$f(1, n-1) = f(2, n) = f(n, 2)$$

d. h. die Partialquotienten

$$a_1, a_2, a_3, a_4, \dots a_{n-2}, a_{n-1}$$

müssen dieselbe (Zähler-) Function geben, als die Partialquotienten

$$a_n, a_{n-1}, a_{n-2}, a_{n-3} \dots a_3, a_2.$$

Dieses wird auf jeden Fall eintreten, wenn

$$a_1 = a_n, a_2 = a_{n-1}, a_3 = a_{n-2}, \dots a_{n-1} = a_2$$

ist und wir kommen somit auf folgende bemerkenswerthe Form eines Kettenbruches

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots\dots + \frac{1}{a_4 + \frac{1}{a_3 + \frac{1}{a_2 + \frac{1}{a_1}}}}}}}.$$

Ein solcher Kettenbruch, in welchem die Ordnung seiner Elemente oder Partialquotienten ohne Veränderung seines Werthes umgekehrt werden kann, heisst ein **symmetrischer Kettenbruch**.

Wir haben die Berechtigung mit unendlichen Kettenbrüchen zu rechnen oben nachgewiesen und es erscheint daher angemessen, ein Beispiel

dieser Rechnung zu geben. Zu dem Zwecke wollen wir die sogenannten periodischen Kettenbrüche, d. h. solche Kettenbrüche, in denen eine gewisse Reihe von Partialquotienten beständig wiederkehrt, einer speciellen Discussion unterwerfen. Da ein solcher Kettenbruch, wie wir gezeigt haben, immer einer endlichen und bestimmten Quantität gleich ist, so wollen wir dieselbe gleich x setzen und gehen mithin von der Gleichung

$$x = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots\dots\dots + \frac{1}{a_n + a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots\dots + \frac{1}{a_n + a_1 + \frac{1}{a_2 + \dots}}}}}}}$$

aus, die wir auch durch die folgende ersetzen können:

$$x = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots\dots + \frac{1}{a_n + x}}}}$$

Denken wir uns jetzt den $n$ten Näherungsbruch

$$\frac{Z_n}{N_n} = \frac{a_n Z_{n-1} + Z_{n-2}}{a_n N_{n-1} + N_{n-2}}$$

berechnet, so erhalten wir daraus durch Einsetzung von $a_n + x$ an Stelle von a_n den Werth des ganzen Kettenbruches, also

$$x = \frac{(a_n + x)Z_{n-1} + Z_{n-2}}{(a_n + x)N_{n-1} + N_{n-2}} = \frac{xZ_{n-1} + Z_n}{xN_{n-1} + N_n}.$$

Hieraus ergiebt sich die quadratische Gleichung

$$N_{n-1}x^2 + (N_n - Z_{n-1})x - Z_n = 0,$$

welche, da die Zahlen N_n, N_{n-1}, Z_n, Z_{n-1} sämmtlich positiv sind, eine positive und eine negative Wurzel hat. Die negative Wurzel kann unserem gegebenen Kettenbruche keinenfalls gleich sein, und mithin drückt die positive Wurzel den Werth x desselben aus.

Betrachten wir den umgekehrten Kettenbruch

$$y = a_n + \frac{1}{a_{n-1} + \frac{1}{a_{a-2} + \dots\dots + \frac{1}{a_1 + y}}}$$

so findet man, wie vorher

$$y = \frac{yZ'_{n-1} + Z'_n}{yN'_{n-1} + N'_n};$$

nun ist aber

$Z'_n = f(n,1) \quad = f(1,n) \quad = Z_n \quad , Z'_{n-1} = f(n,2) \quad = f(2,n) \quad = N_n,$
$N'_n = f(n-1,1) = f(1,n-1) = Z_{n-1}, \; N'_{n-1} = f(n-1,2) = f(2,n-1) = N_{n-1};$

mithin

$$y = \frac{N_n y + Z_n}{N_{n-1} y + Z_{n-1}},$$

und hieraus bildet man sich wieder die quadratische Gleichung:

$$N_{n-1} y^2 - (N_n - Z_{n-1}) y - Z_n = 0,$$

deren positive Wurzel den Werth des gesuchten Kettenbruches darstellt.

Die quadratische Gleichung für y geht aus der für x hervor, wenn man in letzterer $-x$ an die Stelle von x substituirt. Mithin ist die positive Wurzel der ersten Gleichung, nach ihrem absoluten Werthe genommen, gleich der negativen Wurzel der zweiten Gleichung, und man kommt mithin zu dem Theoreme:

Die quadratische Gleichung

$$N_{n-1} x^2 + (N_n - Z_{n-1}) x - Z_n = 0,$$

wo die Ausdrücke N_n, N_{n-1}, Z_n, Z_{n-1} sich aus den gleichnamigen Näherungsbrüchen des unendlichen periodischen Kettenbruches

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots\ldots + \cfrac{1}{a_n + a_1 + \ldots}}}$$

ergeben, bestimmt durch ihre positive Wurzel den Werth eben dieses Kettenbruches und durch ihre negative Wurzel den absoluten Werth von dessen Umkehrung.

Setzt man $a_n = 0$, so fliesst hieraus das zweite Theorem:

Die quadratische Gleichung

$$N_{n-1} x^2 + (N_{n-2} - Z_{n-1}) x - Z_{n-2} = 0$$

bestimmt durch ihre beiden Wurzeln die absoluten Werthe der beiden Kettenbrüche:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots\ldots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_1 + \ldots}}}}$$

und

$$\cfrac{1}{a_{n-1}+\cfrac{1}{a_{n-2}+\cfrac{1}{a_{n-3}+\ldots\ldots+\cfrac{1}{a_1+\cfrac{1}{a_{n-1}+\ldots\ldots}}}}}$$

und zwar ersteren durch ihre positive, letzteren durch ihre negative Wurzel.

Es ist nämlich in Folge der speciellen Annahme $a_k = 0$

$$N_n = a_n N_{n-1} + N_{n-2} = N_{n-2},$$

$$Z_n = a_n Z_{n-1} + Z_{n-2} = Z_{n-2},$$

und hiermit die letztgenannte quadratische Gleichung aus der vorhergehenden deducirt.

Setzt man dagegen

$$a_n = a_1,\ a_{n-1} = a_2,\ a_{n-2} = a_3,\ \ldots\ldots,$$

so verwandeln sich unsere beiden periodischen Kettenbrüche in einen einzigen mit periodischer Periode, und dem entsprechend muss die gemischte quadratische Gleichung in eine reine übergehen, d. h. es muss

$$N_n = Z_{n-1}$$

werden. In der That ist es leicht, diese Gleichung zu verificiren; denn es ist alsdann

$$N_n = f(2, n) = f(a_2, a_3, a_4, \ldots . a_{n-1}, a_n) = f(a_{n-1}, a_{n-2}, a_{n-3} \ldots . a_2, a_1)$$
$$= f(n-1, 1) = f(1, n-1) = Z_{n-1}.$$

Beispiele:

1) $$2+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{2+\ldots}}}}} = \frac{13+\sqrt{365}}{14}.$$

	2	3	2
1	2	7	16
0	1	3	7.

$$7x^2+(3-16)x-7=0$$
$$x^2-\frac{13}{7}x = 1$$
$$x = \frac{13\pm\sqrt{365}}{14}$$

$$\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{2+\ldots}}}}}} = \frac{-13+\sqrt{365}}{14}.$$

2) $$2+\cfrac{1}{1+\cfrac{1}{2+2+\cfrac{1}{1+\cfrac{1}{2+2+\ldots}}}} = 2+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{4+\ldots}}}} = \sqrt{8}$$

	2	1	2
1	2	3	8
0	1	1	3

$$x^2+(3-3)x-8=0$$
$$x=\sqrt{8}$$

3) $1+\frac{1}{2+\frac{1}{3+1+\frac{1}{2+\frac{1}{3+1+\dots}}}} = 1+\frac{1}{2+\frac{1}{4+\frac{1}{2+\frac{1}{4+\dots}}}} = -1+\sqrt{6}.$ $\begin{array}{c|c|c|c} & 1 & 2 & 3 \\ \hline \frac{1}{0} & \frac{1}{1} & \frac{3}{2} & \frac{10}{7} \end{array}$ $2x^2+(7-3)x-10=0$ $x=-1\pm\sqrt{6}$

$$3+\frac{1}{2+\frac{1}{1+3+\frac{1}{1}}} = 3+\frac{1}{2+\frac{1}{4+\frac{1}{2+\frac{1}{4+\dots}}}} = 1+\sqrt{6}$$

§. 7.

Auflösung der Congruenz $ax \equiv c$ (*mod b*) mit Anwendung der Kettenbrüche.

1) Zwei auf einander folgende Näherungsbrüche haben bekanntlich die Eigenschaft, dass, im Falle sie zu einem ächten Bruche gehören,

$$Z_m N_{m-1} - Z_{m-1} N_m = (-1)^{m-1}$$

und, im Falle dass sie zu einem unächten Bruche gehören,

$$Z_m N_{m-1} - Z_{m-1} N_m = (-1)^m$$

ist. Sei nun $\frac{a}{b}$ der Werth des $m$gliedrigen Kettenbruches, so ist

$$Z_m = a,\ N_m = b$$

und $\frac{Z_{m-1}}{N_{m-1}}$ ist der vorletzte Näherungsbruch; die bezeichnete Gleichung geht über in

$$aN_{m-1} - bZ_{m-1} = \begin{cases}(-1)^{m-1}\\(-1)^m\end{cases}$$

und diese Gleichung ist gleichbedeutend mit der Congruenz

$$aN_{m-1} \equiv \begin{cases}(-1)^{m-1}\\(-1)^m\end{cases} \pmod b,$$

aus welcher durch Multiplication mit -1 die zweite folgt:

$$a_1 . -N_{m-1} \equiv \begin{cases}(-1)^m\\(-1)^{m-1}\end{cases} \pmod b.$$

Fasst man beides zusammen, so erhellt, dass die beiden Congruenzen

$$ax \equiv \pm 1 \pmod b$$

auf jeden Fall durch die Zahlen

$$x = \pm N_{m-1}$$

befriedigt werden, und zwar ist jede eine Lösung in der kleinsten positiven oder negativen Zahl, weil zu Folge der Natur der Näherungsbrüche $N_{m-1} < N_m$, also auch $N_{m-1} < b$ ist.

Beispiel 1. Die zu lösende Congruenz sei

$$127x \equiv +1 \ (mod\ 89)$$

```
89 | 127 | 1
     89
     38 | 89 | 2
          76
          13 | 38 | 2
               26
               12 | 13 | 1
                    12
                     1 | 12 | 12
```

	1	2	2	1	12
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{7}{5}$	$\frac{10}{7}$	

$x = 7,\ 127x \equiv 889 \equiv -1\ (mod\ 89)$

Da mithin $x = 7$ der vorgelegten Congruenz nicht genügt, so genügt ihr $x = -7$ oder $x = +82$, und in beiden Fällen ist es leicht, sich davon zu überzeugen.

Beispiel 2. Die aufzulösende Congruenz sei

$$127x \equiv +1 \ (mod\ 153).$$

Die Rechnung ergiebt:

	1	4	1	7	1	2
$\frac{0}{1}$	$\frac{1}{1}$	$\frac{4}{5}$	$\frac{5}{6}$	$\frac{39}{47}$	$\frac{44}{53}$	

Unser m (die Gliederzahl des Kettenbruches) ist hier 6, und mithin, da $\frac{127}{153}$ ein ächter Bruch ist, wenn man $x = 53$ annimmt, $127x \equiv (-1)^{6-1} = -1$, und dem zu Folge

$$x = -53 \text{ oder } +100$$

eine Lösung der vorgelegten Congruenz.

2) Die Lösung der allgemeinen Congruenz

$$ax \equiv c \ (mod\ b),$$

wo c eine nach Belieben positive oder negative Zahl sein kann, führt sich immer auf die Lösung der speciellen Congruenz

$$ax \equiv \pm 1 \ (mod\ b)$$

zurück. Denn, da man

$$\pm c \equiv \pm c \ (mod\ b)$$

hat, so folgt durch Multiplication beider Congruenzen

$$\pm acx \equiv c \pmod{b},$$

und man bekommt mithin eine der beiden Zahlen

$$+cx, \quad -cx$$

als Lösungen der vorgelegten Congruenz, je nachdem der specielle Zahlenwerth

$$x = N_{m-1}$$

den Ausdruck ax mit der Zahl $+1$ oder -1 congruent macht.

Setzen wir die gefundene particuläre Lösung, die entweder eine positive oder negative Zahl sein wird, gleich α, so wird offenbar der Ausdruck

$$x = bn + \alpha$$

die allgemeine Lösung unserer Congruenz darstellen, wenn man darin die Zahl n nach und nach die ganze positive und negative unendliche Zahlenreihe durchlaufen lässt. Es kann vorkommen, dass der absolute Werth von α grösser ist als der Modul b; dann kann man aber immer die Zahl n' so bestimmen, dass die particuläre Lösung

$$bn' + \alpha = \beta$$

kleiner als b ausfällt und der allgemeinen Lösung die Form

$$x = bn + \beta$$

geben, wo wiederum n alle nur möglichen entweder positiven oder negativen ganzen Zahlen bezeichnet.

Beispiel 1. Die aufzulösende Congruenz sei

$$237x \equiv 419 \pmod{179}.$$

Nachdem man die Partialquotienten des Kettenbruches

$$\frac{a}{b} = \frac{237}{179}$$

aufgesucht, findet man die Näherungsbrüche, wie folgt:

	1	3	11	1	1	2
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{4}{3}$	$\frac{45}{34}$	$\frac{49}{37}$	$\frac{94}{71}$	

Die Zahl 71 ist mithin, da $\frac{a}{b}$ hier ein unächter Bruch und die Zahl m dem Partialquotienten gleich 6 ist, eine Lösung der Congruenz

$$237x \equiv (-1)^6 = +1,$$

und darum

$$419 \,.\, 71 = 166 \,.\, 179 + 35 \equiv 35$$

eine particuläre Lösung der vorgelegten Congruenz. Mithin ist die all-

$$x = 179n + 35.$$

In der That ist es leicht sich zu überzeugen, dass $237 \,.\, 35$ und 419 in Bezug auf den Modul 179 denselben Rest lassen, nämlich 61.

Beispiel 2. Die aufzulösende Congruenz sei

$$131x \equiv 98 \ (mod\ 86).$$

Die Näherungsbrüche von $\frac{131}{86}$ werden

	1	1	1	10	4
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{32}{21}$	

und da $\frac{131}{86}$ unächt und $m = 5$, so ist 21 eine Lösung der Congruenz $131x \equiv (-1)^5 = -1$, und mithin

$$-98 \,.\, 21 = 24 \,.\, 86 + 6 \equiv 6$$

eine particuläre Lösung der vorgegebenen Congruenz. Die allgemeine heisst demgemäss

$$x = 86n + 6 \text{ oder } = 86n - 80.$$

Als Rechnungsbeispiele mögen noch folgende Congruenzen mit den nebenstehenden Auflösungen dienen:

$$17x \equiv 3 \ (mod\ 39), \ x = 39n - 9,$$
$$31x \equiv 2 \ (mod\ 13), \ x = 13n + 3,$$
$$47x \equiv 4 \ (mod\ 15), \ x = 15n + 2,$$
$$37x \equiv 4800 \ (mod\ 51), \ x = 51n + 36.$$

Es bedarf wohl kaum der Wiederholung der Bemerkung, dass man die Auflösung irgend einer Congruenz in Consequenz der eingeführten Bezeichnung wieder als Congruenz sich schreiben kann. Die Auflösung der 4 letztgenannten Congruenzen erhalten hiernach folgende Form:

$$x \equiv -9 \ (mod\ 39),$$
$$x \equiv 3 \ (mod\ 13),$$
$$x \equiv 2 \ (mod\ 15),$$
$$x \equiv 36 \ (mod\ 51).$$

3) Bei der Auflösung von Congruenzen kann zuweilen folgender Satz eine nützliche Anwendung finden, vermöge dessen eine auf einen zusammengesetzten Modul bezogene Congruenz sich auf soviele zu dessen Primfactoren bezogene Congruenzen zurückführen lässt, als überhaupt solche da sind:

Es mögen die Zahlen

$$\alpha,\ \beta,\ \gamma,\ \delta,\ \dots\dots\dots\ \mu,\ \nu$$

ch einander als particuläre Lösungen der n Congruenzen

$$\begin{aligned} Ax + C &\equiv 0 \ (mod\ a), \\ Ax + C' &\equiv 0 \ (mod\ b), \\ Ax + C'' &\equiv 0 \ (mod\ c), \\ Ax + C''' &\equiv 0 \ (mod\ d), \\ &\dots\dots \\ &\dots\dots \\ Ax + C^{(n-1)} &\equiv 0 \ (mod\ n) \end{aligned}$$

stimmt sein, in denen die C vermöge der Gleichungen

$$= \frac{A\alpha + C}{a},\ C'' = \frac{A\beta + C'}{b},\ C''' = \frac{A\gamma + C''}{c},\ \dots\dots\ C^{(n-1)} = \frac{A\mu + C^{(n-2)}}{m}$$

ch und nach aus der ersten Congruenz ableitbar sind: als- nn ist der Ausdruck

$$\alpha + a\beta + ab\gamma + abc\delta + \dots\dots\dots + abc\dots.m\nu$$

ne particuläre Lösung der Congruenz:

$$Ax + C \equiv 0 \ (mod\ abcd\dots.mn).$$

Wir wollen den Beweis, da er mit grosser Leichtigkeit sich verallge- einern lässt, blos auf 4 Factoren beziehen, und bemerken zuerst, dass die alle ganze Zahlen sind. Betrachten wir z. B. C''', so ist vermöge der rhergehenden Congruenz, welcher γ genügen soll,

$$A\gamma + C'' \equiv 0 \ (mod\ c),$$

h. aber nichts anderes als:

$$C''' = \frac{A\gamma + C''}{c} = Intg.$$

n nun den eigentlichen Satz zu beweisen, haben wir nur darzuthun, dass r Ausdruck

$$\frac{A(\alpha + a\beta + ab\gamma + abc\delta) + C}{abcd}$$

ı ganzer Quotient ist. Dies trifft aber offenbar zu, denn man kann ihm ıch einander folgende Formen geben:

$$\frac{A(bc\delta + b\gamma + \beta) + \dfrac{A\alpha + C}{a}}{bcd} = \frac{A(bc\delta + b\gamma + \beta) + C'}{bcd},$$

$$\frac{A(c\delta+\gamma)+\frac{A\beta+C'}{b}}{cd}=\frac{A(c\delta+\gamma)+C''}{cd},$$

$$\frac{A\delta+\frac{A\gamma+C''}{c}}{d}=\frac{A\delta+C'''}{d}=Intg.$$

Beispiel. Die aufzulösende Congruenz sei

$$101x \equiv 353 \ (mod\ 2520).$$

Da man durch Zerlegung des Moduls in seine Factoren

$$2520 = 2^3 . 3^2 . 5 . 7$$

findet, so kann man die Congruenz auf $(3+2+1+1) = 7$ einfachere Congruenzen zurückführen; indessen, wenn wir statt der drei auf den Modul 2 bezogenen eine einzige einführen, die sich auf den Modul 8 bezieht, so erniedrigt sich diese Anzahl auf 5. Die Rechnung gestaltet sich, wenn man durch Absonderung der Vielfachen der respectiven Moduls auf beiden Seiten der verschiedenen Congruenzen ihnen die möglichst einfache Form giebt, wie folgt:

(1) $101x-353 \equiv 0 \ (mod\ 8)$
$5x-\ \ 1 \equiv 0$
$\alpha=5, C'=\frac{101.5-353}{8}=19$
$a=8.$

(2) $101x+19 \equiv 0 \ (mod\ 3)$
$2x+\ 1 \equiv 0$
$\beta=1,\ C''=\frac{101.1+19}{3}=40$
$b=3.$

(3) $101x+40 \equiv 0 \ (mod\ 3)$
$2x+\ 1 \equiv 0$
$\gamma=1,\ C'''=\frac{101+40}{3}=47$
$c=3.$

(4) $101x+47 \equiv 0 \ (mod\ 5)$
$x+\ 2 \equiv 0$
$\delta=3,\ C^{IV}=\frac{101.3+47}{5}=70$
$d=5.$

(5) $101x+70 \equiv 0 \ (mod\ 7)$
$3x \equiv 0,\ \varepsilon=0.$

Hiernach findet man

$$\alpha+a\beta+ab\gamma+abc\delta+abcd\varepsilon = 5+8+24+72.3+360.0.$$
$$= 253.$$

Die Auflösung der vorgelegten Congruenz ist mithin

$$x \equiv 253 \ (mod\ 2520),$$

und wenn man erwägt, dass man die Rechnung noch mehr hätte abkürzen können durch Zusammenziehung der beiden Congruenzen nach dem Modul 3

in eine einzige nach dem Modul 9, so wird man gestehen, dass sie überraschend schnell und leicht zum Ziele geführt hat. Unser Satz wird überhaupt in allen solchen Fällen die vortheilhafteste Anwendung finden, wo der Modul irgend einer Congruenz sich aus kleinen Primfactoren zusammensetzt, indem die auf solche bezüglichen Congruenzen ohne alle Rechnung durch einfaches Probiren auflösbar sind.

§. 8.

Anwendung der Congruenzen des ersten Grades.

In den vorhergehenden Paragraphen ist die Theorie der Congruenz

$$Ax \equiv C \ (mod\ B)$$

des ersten Grades, wie man sie darum zu nennen pflegt, weil in ihr die Unbestimmte x nur in der 0ten und ersten Potenz vorkommt, vollständig enthalten, und es bleibt daher nur noch übrig, einige der wesentlichsten Anwendungen zu erörtern, welche diese Theorie findet.

1) Unter diesen beginnen wir mit derjenigen, welche sie auf die folgende wichtige Aufgabe findet: Eine Zahl zu finden, welche durch eine Reihe gegebener Zahlen dividirt gegebene Reste lässt.

Hierzu ist aber noch ein Hülfssatz erforderlich, welcher also lautet:

Wenn eine Zahl N durch eine zusammengesetzte Zahl dividirt den Rest a lässt, oder mit anderen Worten, wenn

$$N \equiv a \ (mod\ mn)$$

und wenn ferner die Reste dieser Zahl N in Bezug auf die einzelnen Factoren m und n respective a' und a'' sind, also

$$N \equiv a' \ (mod\ m)$$

und

$$N \equiv a'' \ (mod\ n),$$

so folgt, wofern m und n relative Primzahlen sind,

$$a \equiv a' \ (mod\ m),$$

$$a \equiv a'' \ (mod\ n),$$

oder in Worten: der Hauptrest a ist den Theilresten a' und a'' nach den zugehörigen Divisoren congruent.

Behufs des Beweises bemerke man, dass, wenn α, β und γ ganze Zahlen bezeichnen, aus den gegebenen Congruenzen folgende Gleichungen folgen:

$$N = \alpha mn + a,$$
$$N = \beta m \;\; + a',$$
$$N = \gamma n \;\; + a'';$$

mithin, indem man N aus ihnen eliminirt, nach einigen leichten Umformungen

$$a = (\beta - \alpha n)m + a',$$
$$a = (\gamma - \alpha m)n + a'',$$

und hieraus folgen unmittelbar die in Frage stehenden Congruenzen.

Nehmen wir also zunächst an, dass die gegebenen Divisoren

$$a,\; a_1,\; a_2,\; a_3,\; \ldots\ldots$$

Primzahlen unter sich sind, und suchen uns nun diejenige Zahl N zu bestimmen, welche durch diese a dividirt die Reste

$$r,\; r_1,\; r_2,\; r_3,\; \ldots\ldots$$

lässt. Dann kann man, in Folge der vorhergehenden Entwickelungen, immer solche Zahlen

$$m,\; m_1,\; m_2,\; m_3,\; \ldots\ldots$$

finden, welche den Congruenzen

$$m a_1 a_2 a_3 a_4 \;\ldots\ldots \equiv 1 \pmod{a},$$
$$m_1 a a_2 a_3 a_4 \;\ldots\ldots \equiv 1 \pmod{a_1},$$
$$m_2 a a_1 a_3 a_4 \;\ldots\ldots \equiv 1 \pmod{a_2},$$
$$m_3 a a_1 a_2 a_4 \;\ldots\ldots \equiv 1 \pmod{a_3},$$
$$\ldots\ldots$$
$$\ldots\ldots$$

Genüge leisten (denn nach der Voraussetzung sind $a_1 a_2 a_3 a_4 \ldots.$ und a, $a a_2 a_3 a_4 \ldots.$ und a_1 u. s. w. relative Primzahlen) und dieses vorausgesetzt wird

$$N = r m a_1 a_2 a_3 a_4 \ldots. + r_1 m_1 a a_2 a_3 a_4 \ldots. + r_2 m_2 a a_1 a_3 a_4 \ldots.$$
$$+ r_3 m_3 a a_1 a_2 a_4 \ldots. + \ldots\ldots$$

Schon der Anblick dieses Werthes zeigt, dass die Division z. B. durch a in sämmtliche Glieder aufgeht, nur in das erste nicht, und da

$$m a_1 a_2 a_3 \ldots. \equiv 1 \pmod{a},$$

so folgt

$$rma_1 a_2 a_3 \ldots. \equiv r \ (mod\ a)$$

oder der Divisionsrest in das erste Glied und mithin in N überhaupt ist r. Dieses Raisonnement wiederholt sich für jedes andere a und der gefundene Zahlenausdruck N leistet mithin den Bedingungen der Aufgabe Genüge.

Wenn die Zahl N der Aufgabe genügt, so müssen es auch die unendlich vielen Zahlen, welche der N nach dem Modul $aa_1a_2a_3a_4 \ldots.$ congruent sind. Denn sie alle lassen durch $aa_1a_2a_3 \ldots.$ dividirt den Rest N und da ferner nach dem vorangestellten Hülfssatze die Reste, welche irgend eine von ihnen durch die Divisoren a, a_1, a_2, a_3, ... lässt, dieser Zahl N nach eben denselben Divisoren congruent sind, so müssen diese Reste dieselben sein wie die der Zahl N, d. h. sie fallen mit den gegebenen Resten zusammen.

Sei z. B.

$$a=3,\ a_1=7,\ a_2=10,$$

$$r=2,\ r_1=3,\ r_2=9,$$

so sind die aufzulösenden Congruenzen

$$70m \equiv 1 \ (mod\ 3),$$

$$30m_1 \equiv 1 \ (mod\ 7),$$

$$21m_2 \equiv 1 \ (mod\ 10),$$

denen Genüge geschieht durch die Annahmen

$$m \equiv 1 \ (mod\ 3),$$

$$m_1 \equiv 4 \ (mod\ 7),$$

$$m_2 \equiv 1 \ (mod\ 10);$$

mithin folgt die particuläre Lösung

$$N = 2.1.7.10 + 3.4.3.10 + 9.1.3.7 = 689$$

und die allgemeine

$$N \equiv 689 \ (mod\ 210).$$

Die kleinste Zahl, welche hierunter begriffen ist, ist

$$N = 689 - 3.210 = 59$$

und man kann daher die Congruenz, welcher N genügen muss, auch einfacher, wie folgt, schreiben:

$$N \equiv 59 \ (mod\ 210).$$

Wenn a, a_1, a_2, a_3, ... keine Primzahlen unter sich sind, so zerlegt man sie in ihre einzelnen Primfactoren und kommt dadurch auf den vorigen Fall wieder zurück: es ist dann aber allemal eine gewisse Auf-

merksamkeit auf die Untersuchung zu wenden, ob die gestellte Aufgabe möglich und zulässig ist, oder ob sie sich selber widerspricht. Haben wir z. B.

$$a = 6, \ a_1 = 12, \ a_2 = 15$$

und die entsprechenden Reste

$$r = 1, \ r_1 = 1, \ r_2 = 10,$$

so können wir zunächst 6 ganz und gar unberücksichtigt lassen. Denn wenn eine Zahl durch 12 dividirt 1 zum Reste lässt, so bleibt derselbe Rest auch bei der Division mit 6. Jede Zahl nun, welche durch 12 divirdirt den Rest 1 hat, ist von der Form

$$3 \,.\, 4n + 1$$

und lässt also ebensowohl für 3 als auch für 4 den Rest 1. Ferner die Zahlen, welche nach dem Modul 15 den Rest 10 geben, sind von der Form

$$3 \,.\, 5n + 10$$

und dividiren wir hier durch 3, so erkennen wir, dass, in Uebereinstimmung mit dem Vorigen, der Rest 1 bleibt; die Division dagegen durch 5 giebt den Rest 0. Demgemäss reducirt sich jetzt die Aufgabe derartig, dass

$$a = 3, \ a_1 = 4, \ a_2 = 5,$$
$$r = 1, \ r_1 = 1, \ r_2 = 0.$$

und die aufzulösenden Congruenzen sind

$$20m \equiv 1 \ (mod\ 3),$$
$$15m_1 \equiv 1 \ (mod\ 4),$$
$$12m_2 \equiv 1 \ (mod\ 5).$$

Diesen Congruenzen wird genügt durch

$$m \equiv 2 \ (mod\ 3),$$
$$m_1 \equiv 3 \ (mod\ 4),$$
$$m_2 \equiv 3 \ (mod\ 5).$$

Mithin wird

$$N = 1.2.20 + 1.3.15 + 0.3.12 = 85$$

und allgemein

$$N \equiv 85 \text{ oder } \equiv 25 \ (mod\ 25).$$

Als zweites Beispiel nehmen wir an:

$$a = 4, \ 6, \ 9, \ 15,$$
$$r = 3, \ 3, \ 3, \ 12.$$

Wir bekommen zunächst als mit dem Vorigen gleichgeltend

$$a = 4, \ 2, \ 3, \ 9, \ 3, \ 5,$$
$$r = 3, \ 3, \ 3, \ 3, \ 12, \ 12,$$

und erkennen, dass kein Widerspruch in der Aufgabe ist; denn wenn dem Modul der Rest 3 entspricht, so muss 2 gleichfalls diesen Rest geben; und wenn wir zu 3 die beiden Reste 3 und 12 haben, so sind diese gleichbedeutend, nämlich gleich 0. Streifen wir alles Ueberflüssige ab, so bekommen wir folgende reducirte Form unserer Aufgabe:

$$a = 4,\ 9,\ 5$$
$$r = 3,\ 3,\ 2$$

und die folgenden Congruenzen zu lösen:

$$45m \equiv 1 \ (mod\ 4),$$
$$20m_1 \equiv 1 \ (mod\ 9),$$
$$36m_2 \equiv 1 \ (mod\ 5);$$

die Auflösungen sind

$$m \equiv 1 \ (mod\ 4),$$
$$m_1 \equiv 5 \ (mod\ 9),$$
$$m_2 \equiv 1 \ (mod\ 5)$$

und ergeben den particulären Werth von N

$$N = 3.1.45 + 3.5.20 + 2.1.36 = 507$$

oder, wenn man die Vielfachen von $4.9.5 = 180$ absondert,

$$= 147.$$

Mithin ist die allgemeine Lösung

$$N \equiv 147 \text{ oder } \equiv -33 \ (mod\ 180).$$

2) Einen gegebenen Bruch in mehrere Partialbrüche zu zerlegen, deren Nenner die einzelnen Factoren von dem Nenner des gegebenen Bruches sind.

Wenn man die Gleichung

$$\frac{N}{aa_1a_2a_3 \ldots\ldots} = \frac{X}{a} + \frac{X_1}{a_1} + \frac{X_2}{a_2} + \frac{X_3}{a_3} + \ldots\ldots$$

setzt, so folgt augenblicklich

$$N = Xa_1a_2a_3 \ldots\ldots + X_1aa_2a_3 \ldots\ldots + X_2aa_1a_3 \ldots\ldots + X_3aa_1a_2a_4 \ldots\ldots$$

und die Bedingungsgleichungen dafür, dass diese Gleichung bestehe, sind

$$N \equiv Xa_1a_2a_3a_4 \ldots\ldots (mod\ a),$$
$$N \equiv X_1aa_2a_3a_4 \ldots\ldots (mod\ a_1),$$
$$N \equiv X_2aa_1a_3a_4 \ldots\ldots (mod\ a_2),$$
$$N \equiv X_3aa_1a_2a_4 \ldots\ldots (mod\ a_3).$$

. . . . . .

. . . . . .

Die Auflösung dieser Congruenzen giebt die Zahlform für die einzelnen Partialnenner.

Beispiel. Es sei

$$\frac{523}{3.5.7.8} = \frac{523}{840} = \frac{X}{3} + \frac{X_1}{5} + \frac{X_2}{7} + \frac{X_3}{8};$$

dann sind die aufzulösenden Congruenzen

$$523 \equiv 280X \ (mod\ 3),$$
$$523 \equiv 168X_1 \ (mod\ 5),$$
$$523 \equiv 120X_2 \ (mod\ 7),$$
$$523 \equiv 105X_3 \ (mod\ 8)$$

oder, wenn man, indem man überall mit dem respectiven Modul auf beiden Seiten dividirt, die kleinsten Reste nimmt und ausserdem noch die auf diese Weise aus der zweiten fliessende Congruenz

$$3 \equiv 3X_1 \ (mod\ 5)$$

noch durch die Division mit 3 auf beiden Seiten vereinfacht (diese Division ist, da 3 und 5 relative Primzahlen sind, statthaft nach §. 4, 4) einfacher

$$1 \equiv X \ (mod\ 3),$$
$$1 \equiv X_1 \ (mod\ 5),$$
$$2 \equiv X_2 \ (mod\ 7),$$
$$3 \equiv X_3 \ (mod\ 8).$$

Mithin haben wir durch diese Transformation geradezu die Auflösungen der vorhergehenden Congruenzen bestimmt, und wir erhalten nun durch Substitution der Werthe der X in die Ausgangsgleichung

$$\frac{523}{840} = \frac{1}{3} + \frac{1}{5} - \frac{2}{7} + \frac{3}{8} = \frac{280+168+240+315}{840}.$$

Man überzeugt sich leicht, dass, wenn man die Bedingung stellt, dass die Partialbrüche nur ächt sein dürfen, die Anzahl der Lösungen eine beschränkte ist, nämlich das letzte Glied $\frac{3}{8}$ darf nicht vergrössert werden, weil es sonst ein unächter Bruch würde; wohl aber kann man es um eine Einheit verkleinern, wodurch $-\frac{5}{8}$ kommt; von den übrig bleibenden Gliedern ist dann $-\frac{2}{7}$ das einzige, welches eine Vergrösserung gestattet. Wir bekommen also

$$\frac{523}{840} = \frac{1}{3} + \frac{1}{5} + \frac{5}{7} - \frac{5}{8}.$$

Was ferner das vorletzte Glied $-\frac{2}{7}$ anbetrifft, so gestattet es nur eine

Vergrösserung um 1 und man hat dann die Wahl entweder $\frac{1}{3}$ oder $\frac{4}{5}$ um 1 zu verkleinern; dies giebt also zwei weitere Lösungen

$$\frac{523}{840} = +\frac{1}{3} - \frac{4}{5} + \frac{5}{7} + \frac{3}{8},$$
$$\frac{523}{840} = -\frac{2}{3} + \frac{1}{5} + \frac{5}{7} + \frac{3}{8}.$$

Andere Auflösungen als diese vier sind unmöglich.

3) In dem Vorstehenden haben wir die Theorie der Congruenzen mit einer Unbestimmten erörtert. Es bleibt noch übrig von den Congruenzen mit mehreren Unbekannten zu handeln und wir wollen dieses in unmittelbarem Anschluss an Gauss thun, der in seinen berühmten „Disquisitiones arithmeticae" das Nothwendigste über diesen Gegenstand zusammengefasst hat.

Seien die Congruenzen

$$\left.\begin{aligned} ax + by + cz + \ldots\ldots &\equiv g \\ a'x + b'y + c'z + \ldots\ldots &\equiv g' \\ a''x + b''y + c''z + \ldots\ldots &\equiv g'' \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{aligned}\right\} \bmod m$$

gegeben, deren Anzahl n der Zahl der Unbekannten gleich sein möge. Wir multipliciren diese Congruenzen der Reihe nach auf beiden Seiten mit den unbestimmten Factoren ξ, ξ', ξ'' ...., addiren die Producte zusammen und setzen die Coefficienten aller Unbekannten bis auf x der Null gleich, also

$$b\xi + b'\xi' + b''\xi'' + \ldots = 0,$$
$$c\xi + c'\xi' + c''\xi'' + \ldots = 0,$$
$$\ldots\ldots\ldots$$
$$\ldots\ldots\ldots$$

Dann ist aus der Theorie der linearen Gleichungen her bekannt, dass wir die $(n-1)$ Quotienten

$$\frac{\xi'}{\xi}, \frac{\xi''}{\xi}, \frac{\xi'''}{\xi}, \frac{\xi^{IV}}{\xi}, \ldots$$

vermöge der vorhergehenden $(n-1)$ Gleichungen bestimmen und, indem wir der Grösse ξ passend annehmen, immer solche ganzzahligen Werthe der ξ, ξ', ξ'', ξ''', ... erhalten können, welche keinen gemeinschaftlichen Theiler besitzen. Mithin werden aus der vorhin resultirenden Con-

gruenz alle Unbekannten bis auf x herausgehen und die darin vorkommenden ξ lauter bestimmte Zahlengrössen sein.

Weiter multipliciren wir die n gegebenen Congruenzen mit den unbestimmten Factoren η, η', η'', η''',....., addiren die Producte zusammen und setzen die Coefficienten aller Unbekannten bis auf y gleich 0: dann resultirt eine Congruenz, in der allein die Unbekannte y vorkommt und die sonst darin enthaltenen Grössen η sich vermöge der Gleichungen

$$a\eta + a'\eta' + a''\eta'' + \ldots\ldots = 0$$
$$c\zeta + c'\zeta' + c''\zeta'' + \ldots\ldots = 0$$
$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$
$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

als ganze Zahlen bestimmen lassen, welche keinen gemeinschaftlichen Theiler besitzen.

In ähnlicher Weise leitet man eine Gleichung her, in der blos z und die verschiedenen ζ vorkommen, welche vermöge der Gleichungen

$$a\zeta + a'\zeta' + a''\zeta'' + \ldots.$$
$$b\zeta + b'\zeta' + b''\zeta'' + \ldots.$$
$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$
$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

ihre Bestimmung erhalten.

Indem man in dieser Weise fortgeht, ist klar, dass aus den gegebenen Congruenzen sich n andere ableiten lassen, in deren jeder nur je eine Unbekannte vorkommt, nämlich

$$(a\xi + a'\xi' + a''\xi'' + \ldots.)\,x \equiv g\xi + g'\xi' + g''\xi'',$$
$$(b\eta + b'\eta' + b''\eta'' + \ldots.)\,y \equiv g\eta + g'\eta' + g''\eta'',$$
$$(c\eta + c'\eta' + c''\eta'' + \ldots.)\,z \equiv g\zeta + g'\zeta' + g''\zeta''$$
$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$
$$\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot$$

oder wenn wir, grösserer Kürze halber, das Summenzeichen einführen,

$$\left.\begin{array}{l} x\Sigma a\xi \equiv \Sigma g\xi, \\ y\Sigma b\eta \equiv \Sigma g\eta, \\ z\Sigma c\zeta \equiv \Sigma g\zeta, \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot \end{array}\right\} (mod\ m)$$

und die Aufgabe ist mithin auf die Auflösung von Congruenzen mit nur einer Unbekannten zurückgeführt.

Es sind aber jetzt mehrere Fälle zu unterscheiden. Zunächst nämlich können alle Coefficienten der Unbekannten, also die Summenausdrücke: $\Sigma a\xi$, $\Sigma b\eta$, $\Sigma c\zeta$, ... ohne Ausnahme relative Primzahlen zu dem Modul m sein. Alsdann sind die resultirenden Congruenzen sämmtlich nach den vorhergehenden Entwickelungen auflösbar und die n Lösungen derselben sind zu gleicher Zeit die n Lösungen der vorgegebenen Congruenzen.

Es können aber auch zweitens nicht alle Coefficienten der $x, y, z, \ldots.$ zu dem Modul m relative Primzahlen sein, sondern entweder alle oder doch zum Theil irgend welche Factoren $\alpha, \beta, \gamma, \ldots.$ mit m gemeinschaftlich haben. Dann erhellt, dass, wenn die respectiven rechten Seiten unserer Congruenzen nicht durch die nämlichen Factoren theilbar sind, dieselben unmöglich sind: die vorgegebenen Congruenzen sind mithin mit sich selber im Widerspruch.

Wenn dagegen die rechten Seiten diese Division zulassen, so bekommen wir eine Anzahl von Congruenzen nach den Moduln $\frac{m}{\alpha}, \frac{m}{\beta}, \frac{m}{\gamma}, \ldots..$ und deren Auflösung ergiebt:

$$x \equiv A\left(mod\ \frac{m}{\alpha}\right),$$
$$y \equiv B\left(mod\ \frac{m}{\beta}\right),$$
$$z \equiv C\left(mod\ \frac{m}{\gamma}\right),$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

und diese Congruenzen müssen die vollständige Auflösung des gegebenen Systems von Congruenzen enthalten. Nun aber lassen sich dieselben wie folgt schreiben:

$$x \equiv A,\ A+\frac{m}{\alpha},\ A+\frac{2m}{\alpha},\ \ldots..\ A+\frac{(\alpha-1)m}{\alpha}\left(mod\ \frac{m}{\alpha}\right),$$
$$y \equiv B,\ B+\frac{m}{\beta},\ B+\frac{2m}{\beta},\ \ldots..\ B+\frac{(\beta-1)m}{\beta}\left(mod\ \frac{m}{\beta}\right),$$
$$z \equiv C,\ C+\frac{m}{\gamma},\ C+\frac{2m}{\gamma},\ \ldots..\ C+\frac{(\gamma-1)m}{\gamma}\left(mod\ \frac{m}{\gamma}\right),$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

Hier sind die Zahlen

$$A,\ A+\frac{m}{\alpha},\ A+\frac{2m}{\alpha},\ \ldots.\ A+\frac{(\alpha-1)m}{\alpha}$$

nach dem Modul m alle von einander verschieden; denn wären zwei von ihnen einander congruent, so müssten sie sich um irgend ein Vielfaches von m von einander unterscheiden, welches ein offenbarer Widerspruch, da dieser Unterschied mit Nothwendigkeit ein ächter Bruch ist. Da Aehnliches von den übrigen Congruenzen gilt, erhellt jetzt, dass wir für x, y, z, ... respective α, β, γ, ... von einander nach dem Modul m verschiedene Congruenzen erhalten, deren Modul respective $\frac{m}{\alpha}$, $\frac{m}{\beta}$, $\frac{m}{\gamma}$, ... sein werden. Offenbar wenn die vorgelegten Congruenzen möglich sind, so müssen ihre Lösungen unter diesen verschiedenen Congruenzen mit inbegriffen sein; aber es ist durchaus nicht umgekehrt nothwendig, dass alle jene Congruenzen nach $\frac{m}{\alpha}$, $\frac{m}{\beta}$, $\frac{m}{\gamma}$, ... mit den gegebenen identificirt werden können. Im Gegentheil, meistentheils werden nicht alle Werthe von x, y, z, ... mit einander zu combiniren sein, sondern nur gewisse bestimmte, deren Zusammenhang durch gewisse Bedingungscongruenzen ausgedrückt wird. Wie diese Bedingungscongruenzen sich im Allgemeinen ergeben, wollen wir hier nicht näher erörtern, sondern, da wir in den nachfolgenden Untersuchungen dessen nicht bedürfen, uns damit begnügen, in einzelnen Beispielen den allgemeinen Gang zu zeigen, der hierbei einzuschlagen ist.

Beispiel 1. Die gegebenen Congruenzen seien

$$\left.\begin{array}{l} 3x+5y+\ z\equiv 4 \\ 2x+3y+2z\equiv 7 \\ 5x+\ y+3z\equiv 6 \end{array}\right\}\ (mod\ 12).$$

Die Gleichungen für die ξ, η, ζ werden folgende:

$$\begin{array}{lcl} 5\xi+3\xi'+\ \xi''=0 & \text{und} & \xi+2\xi'+3\xi''=0, \\ 3\eta+2\eta'+5\eta''=0 & \text{und} & \eta+2\eta'+3\eta''=0, \\ 3\zeta+2\zeta'+5\zeta''=0 & \text{und} & 5\zeta+3\zeta'+\ \zeta''=0. \end{array}$$

Aus diesen folgt

$$\begin{array}{lll} \xi=\ 1, & \xi'=-2, & \xi''=\ 1, \\ \eta=\ 1, & \eta'=\ 1, & \eta''=-1, \\ \zeta=-13, & \zeta'=22; & \zeta''=-1 \end{array}$$

und mithin wird

$\Sigma a\xi = 3 - 4 + 5 = 4$, $\quad \Sigma b\eta = 5 + 3 - 1 = 7$, $\Sigma c\zeta = -13 + 44 - 3 = 28$

$\Sigma g\xi = 4 - 14 + 6 = -4$, $\Sigma g\eta = 4 + 7 - 6 = 5$, $\Sigma g\zeta = -52 + 154 - 6 = 96$

und die aufzulösenden Congruenzen sind:

$$\left.\begin{aligned} 4x &\equiv -4 \\ 7y &\equiv 5 \\ 28z &\equiv 96 \end{aligned}\right\} (mod\ 12),$$

oder, wenn man den Lehrsatz §. 4, 6) anwendet,

$$\begin{aligned} x &\equiv -1\ (mod\ 3), \\ 7y &\equiv 5\ (mod\ 12), \\ 7z &\equiv 24\ (mod\ 3). \end{aligned}$$

Diesen Congruenzen leisten Genüge

$$\begin{aligned} x &\equiv 2\ (mod\ 3), \\ y &\equiv 11\ (mod\ 12), \\ z &\equiv 0\ (mod\ 3), \end{aligned}$$

oder auch, wenn wir die nach dem Modul 12 verschiedenen Formen aufführen,

$$\begin{aligned} x &\equiv 2,\ 5,\ 8,\ 11\ (mod\ 3), \\ y &\equiv 11\ (mod\ 12), \\ z &\equiv 0,\ 3,\ 6,\ 9\ (mod\ 3). \end{aligned}$$

Um nun zu finden, welche Combinationen zwischen den Werthen von x und z zulässig seien, substituiren wir in die gegebenen Congruenzen für x, y, z die allgemeinen Formen, unter denen sie stehen, nämlich

$$x = 2 + 3x',\ y = 11,\ z = 0 + 3z' = 3z'$$

und erhalten

$$\left.\begin{aligned} 57 + 9x' + 3z' &\equiv 0 \\ 30 + 6x' + 6z' &\equiv 0 \\ 15 + 15x' + 9z' &\equiv 0 \end{aligned}\right\} (mod\ 12).$$

Diesen Congruenzen sind aber, wenn man rechts den Factor 3 herausdividirt, zu Folge des schon öfters angewandten Satzes §. 4, 6) drei andere nach dem Modul 4 gleichgeltend, die, wenn man noch überall die kleinsten Reste nimmt, folgende Darstellung gestatten:

$$\left.\begin{aligned} -(1+x') + z' &\equiv 0 \\ 2(1+x') - 2z' &\equiv 0 \\ (1+x') - z' &\equiv 0 \end{aligned}\right\} (mod\ 4).$$

Die erste und letzte dieser Congruenzen fallen geradezu in eine zusammen; die mittlere drückt eben dieselbe Congruenz aus, aber in allge-

meinerer Weise, nämlich nach dem Modul 2. Wenn also kein Widerspruch eintreten soll, so muss man die Bedingungscongruenz

$$z' \equiv 1+x' \ (mod\ 4)$$

setzen. Die Grössen x' und z' können blos (wenn wir nach dem Modul 12 verschiedene Werthe von x und z erhalten wollen) die Werthe 0, 1, 2, 3 haben und zu Folge der soeben gefundenen Bedingungscongruenz sind folgende Combinationen dieser Werthe zulässig:

$x'=0$ u. $z'=1$, $x'=1$ u. $z'=2$, $x'=2$ u. $z'=3$, $x'=3$ u. $z'=0$

und wir erhalten daher für $x=2+3x'$ die Werthe 2, 5, 8, 11, denen der Reihe nach die Werthe 0, 3, 6, 9 von $z=3z'$ entsprechen, d.h. die Aufgabe lässt 4 von einander (nach dem Modul 12) verschiedene Auflösungen zu, nämlich:

$$\left.\begin{array}{l} x \equiv \ \ 2, \ \ 5, \ \ 8, 11 \\ y \equiv 11, 11, 11, 11 \\ z \equiv \ \ 3, \ \ 6, \ \ 9, \ \ 0 \end{array}\right\} (mod\ 12).$$

Beispiel 2. Die aufzulösenden Congruenzen seien

$$\left.\begin{array}{r} x+3y+4z \equiv \ 5 \\ 2x+\ y+\ z \equiv \ 6 \\ 3x+2y+4z \equiv 13 \end{array}\right\} (mod\ 24).$$

Für die Hülfsgrössen ξ, η, ζ bildet man sich die Gleichungen:

$$3\xi+\ \xi'+2\xi''=0 \text{ und } 4\xi+\xi'+4\xi''=0,$$
$$\eta+2\eta'+3\eta''=0 \text{ und } 4\eta+\eta'+4\eta''=0,$$
$$\zeta+2\zeta'+3\zeta''=0 \text{ und } 3\zeta+\zeta'+2\zeta''=0,$$

aus denen man

$$\xi=-2,\ \xi'=\ \ 4,\ \xi''=1$$
$$\eta=-5,\ \eta'=-8,\ \eta''=7$$
$$\zeta=-1,\ \zeta'=-7,\ \zeta''=5$$

findet. Hierauf bildet man sich weiter

$\Sigma a\xi=-\ 2+\ 8+\ 3=+\ 9$, $\Sigma b\eta=-15-\ 8+14=-9$, $\Sigma c\zeta=-4-7+20=+9$,
$\Sigma g\xi=-10+24+13=+27$, $\Sigma g\eta=-25-48+91=18$, $\Sigma g\zeta=-5-42+65=18$

und hat nun die Congruenzen

$$9x \equiv 27,\ -9y \equiv 18,\ 9z \equiv 18 \ (mod\ 24)$$

aufzulösen. Diesen sind aber folgende gleichgeltend

$$3x \equiv 9,\ 3y \equiv -6,\ 3z \equiv +6 \ (mod\ 8)$$

oder auch wegen §. 4, 6)

$$x \equiv 3,\ y \equiv -2,\ z \equiv +2 \ (mod\ 8).$$

Sucht man die nach dem Modul 24 verschiedenen Congruenzen, welche der Aufgabe Genüge leisten können, so fliessen unmittelbar aus den vorhergehenden die folgenden:

$$\left.\begin{aligned} x &\equiv 3,\ 11,\ 19 \\ y &\equiv -2,\ 6,\ 14 \\ z &\equiv +2,\ 10,\ 18 \end{aligned}\right\} (mod\ 8).$$

Um diejenigen herauszufinden, welche brauchbar sind, bemerken wir, dass sie alle unter den allgemeinen Formen

$$x = 3+8x',\ y = -2+8y',\ z = +2+8z'$$

inbegriffen sind, und setzen diese Werthe in die gegebenen Gleichungen ein, um zu sehen, ob und unter welchen Umständen sie denselben genügen. Aus dieser Substitution resultiren die Congruenzen

$$\left.\begin{aligned} 8x'+24y'+32z' &\equiv 0 \\ 16x'+\ 8y'+\ 8z' &\equiv 0 \\ 24x'+16y'+32z' &\equiv 0 \end{aligned}\right\} (mod\ 24)$$

und diese sind offenbar identisch mit den folgenden:

$$\left.\begin{aligned} x'+3y'+4z' &\equiv 0 \\ 2x'+\ y'+\ z' &\equiv 0 \\ 3x'+2y'+4z' &\equiv 0 \end{aligned}\right\} (mod\ 3),$$

für welche, wenn wir die kleinsten Reste substituiren, auch die folgenden

$$\left.\begin{aligned} x'+z' &\equiv 0 \\ -x'+y'+z' &\equiv 0 \\ -y'+z' &\equiv 0 \end{aligned}\right\} (mod\ 3)$$

genommen werden können. Aus der letzten dieser beiden Gleichungen folgt durch Addition zur zweiten $-x'+2z' \equiv 0$ oder $-x'-z' \equiv 0$ oder $x'+z' \equiv 0$, d. h. die erste Gleichung. Die Subtraction dagegen der zweiten von der dritten liefert $x'-2y' \equiv 0$ oder $x'+y' \equiv 0$ und man sieht jetzt ohne Weiteres ein, dass das System der vorigen 3 Congruenzen identisch dasselbe sei mit dem System der beiden Congruenzen;

$$\left.\begin{aligned} x'+y' &\equiv 0 \\ x'+z' &\equiv 0 \end{aligned}\right\} (mod\ 3)$$

und das sind also die beiden Bedingungscongruenzen, welche von den oben gefundenen Werthen für die x, y, z erfüllt werden müssen, damit sie das System der gegebenen Congruenzen nach dem Modul 24 befriedigen. Man hat für x' die drei Werthe 0, 1, 2 und denen entsprechen wegen der ersten Hülfscongruenz in derselben Reihenfolge die Werthe 0, 2, 1 für y und wegen der zweiten Hülfscongruenz gleichfalls in derselben Reihenfolge dieselben Werthe für z. Dem zu Folge erhalten wir drei von einander verschiedene Lösungen unserer Congruenzen, nämlich

$$\left.\begin{array}{l} x \equiv 3,\ 11,\ 19 \\ y \equiv -2,\ 14,\ 6 \\ z \equiv 2,\ 18,\ 10 \end{array}\right\} (mod\ 24).$$

Man kann übrigens die beiden nach x', y', z' ausgedrückten Hülfscongruenzen auch unmittelbar auf die x, y, z transformiren. Zu dem Zwecke bemerken wir, dass dieselben identisch dasselbe sind, was die Congruenzen

$$\left.\begin{array}{l} 8x'+8y' \equiv 0 \\ 8x'+8z' \equiv 0 \end{array}\right\} (mod\ 24),$$

und substituiren wir hier für $8x'$ seinen Werth $x-3$, für $8y'$ seinen Werth $y+2$ und für $8z'$ seinen Werth $z-2$, so ergeben sich sogleich

$$\left.\begin{array}{l} x+y \equiv 1 \\ x+z \equiv 5 \end{array}\right\} (mod\ 24)$$

als die Bedingungscongruenzen, welche befriedigt werden müssen zu gleicher Zeit mit den obigen, welche x, y, z nach dem Modul 8 bestimmen. Alle solche Combinationen dieser letzteren, welche den ersteren kein Genüge leisten, erfüllen wohl das gegebene Congruenzensystem nach dem Modul 8, aber nicht nach dem Modul 24. Dieses vorausgesetzt sind unter den 27 von einander verschiedenen Combinationen der x, y, z, welche zwischen den ursprünglichen Congruenzen für diese Grössen gebildet werden können, überhaupt nur 3 zulässig, als die einzigen, welche den beiden Bedingungscongruenzen genügen; es sind diese die obigen drei, und in der That verificiren sich rücksichtlich derselben die Congruenzen:

$$\left.\begin{array}{l} 3-2 \equiv 1,\ \ 3+2 \equiv 5 \\ 11+14 \equiv 1,\ 11+18 \equiv 5 \\ 19+6 \equiv 1,\ 19+10 \equiv 5 \end{array}\right\} (mod\ 24).$$

Stellen wir die sich aus unserer dreifachen Auflösung ergebenden positiven Werthe der x, y, z zusammen, so bekommen wir folgende Reihen zusammengehöriger Zahlenwerthe:

$x =\ \ 3\ \ 11\ \ 19\ \ 27\ \ 35\ \ 43\ \ 51\ \ 59\ \ 67\ \ 75\ \ 83\ \ 91\ \ldots\ldots$

$y = -2\ \ 14\ \ 6\ \ 22\ \ 38\ \ 30\ \ 46\ \ 62\ \ 54\ \ 70\ \ 86\ \ 78\ \ldots\ldots$

$z =\ \ 2\ \ 18\ \ 10\ \ 26\ \ 42\ \ 34\ \ 50\ \ 66\ \ 58\ \ 74\ \ 90\ \ 82\ \ldots\ldots,$

von denen je drei einander entsprechende Glieder der drei gegebenen Congruenzen Genüge thun.

Zweiter Abschnitt.

Von den Resten der Potenzen.

§. 9.

Wenn man eine rationale ganze Function von x der $n$ten Ordnung hat, worin die Coefficienten ganze Zahlen sind, entweder positive oder negative: so giebt es höchstens n verschiedene Werthe von x, welche in diese Function substituirt Zahlen geben, die durch eine gegebene Primzahl aufgehen oder gewisse Reste lassen.

Es sei X eine rationale ganze Function von x und man soll die Congruenz

$$X \equiv 0 \pmod p$$

auflösen; es möge der specielle Werth

$$x \equiv a' \pmod p$$

eine Wurzel der Congruenz sein und A' der Werth, den man erhält, wenn man in X statt x seinen Werth a' substituirt, so dass natürlich

$$A' \equiv 0 \pmod p$$

sein muss; es wird daher auch durch Subtraction dieser Congruenz von der gegebenen

$$X - A' \equiv 0 \pmod p.$$

Nun ist ja aber X von der Form

$$X = mx^n + m'x^{n-1} + m''x^{n-2} + \ldots\ldots + m^{(n-1)}x + m^{(n)}$$

und mithin

$$A = ma'^n + m'a'^{n-1} + m''a'^{n-2} + \ldots\ldots + m^{(n-1)}a' + m^{(n)},$$

es ergiebt sich hieraus

$$X - A = m(x^n - a'^n) + m'(x^{n-1} - a'^{n-1}) + m''(x^{n-2} - a'^{n-2}) + \ldots\ldots + m^{(n-1)}(x - a')$$

und da jedes Glied der rechten Seite nach einem bekannten algebraischen Theorem den Factor $x-a'$ enthält, so kann man offenbar, indem man unter X' eine ganze rationale Function der Grösse x vom $(n-1)$ten versteht, setzen

$$X-A' = (x-a')X'.$$

Die letzte Congruenz geht demgemäss über in

$$(x-a')\,X' \equiv 0 \;(mod\,p),$$

welcher, da p eine Primzahl sein soll, nur so genügt werden kann, dass entweder $x-a'$ oder X' durch p aufgeht. Es war aber $x \equiv a$, also $x-a$ durch p ohne Rest dividirbar; soll also der vorgelegten Congruenz ein von a' nach dem Modul p verschiedener Werth der Grösse x genügen, so muss nothwendig

$$X' \equiv 0 \;(mod\;p)$$

sein. Hier wiederholt sich nun dasselbe Raisonnement; wenn es einen Werth

$$x \equiv a'' \;(mod\;p)$$

giebt, für welchen x' der 0 congruent wird, so kommt man wieder auf einen Ausdruck X'' der nächst niedrigeren, nämlich der $(n-2)$ten, Dimension und, wenn die vorgegebene Congruenz von a' und a'' verschiedene Wurzeln hat, so müssen diese auch der Congruenz

$$X'' \equiv 0 \;(mod\;p)$$

genügen. Indem es so weiter fortgeht, bekommen wir schliesslich eine Congruenz des ersten Grades, nämlich

$$X^{(n-1)} = mx + c \equiv 0 \;(mod\;p).$$

Der Coefficient von x muss hier gleich m sein, weil der höchste Coefficient in den Ausdrücken X', X'', X''' ..... zu Folge der Natur ihrer Bildung überall m bleibt, und man darf zu gleicher Zeit annehmen, dass m kein Vielfaches der Primzahl p ist, weil sonst das Glied mx^n in dem Ausdrucke X für sich allein der Null nach dem Modul p congruent und mithin ein überflüssiger Zusatz wäre, den man ohne Weiteres durch Subtraction beseitigen könnte, so dass die betrachtete Congruenz des $n$ten Grades in eine vom $(n-1)$ten Grade überginge. Also ist m eine relative Primzahl zu p. Nun haben wir aber im Vorigen bewiesen, dass, unter der Voraussetzung, dass m und p relative Primzahlen sind, die Congruenz

$$mx+c \equiv 0 \text{ oder } mx \equiv -c \;(mod\;p)$$

des ersten Grades nur eine einzige Lösung zulassen; mithin folgt, dass unsere Congruenz X höchstens n von einander verschiedene Wurzeln haben kann, wenn wir, der Analogie gemäss, unter Wurzeln solche Zahlen verstehen, welche für x eingesetzt den Ausdruck X nach dem Modul p der Null congruent machen. Darum ist es aber noch durchaus nicht nothwendig, dass immer n nach dem Modul p von einander verschiedene Congruenzen wirklich existiren, durch die der Congruenz $X \equiv 0$ Genüge geschieht; denn dies hängt offenbar davon ab, ob sich unter allen Umständen Zahlen auffinden lassen, welche den Congruenzen

$$X', X'', X''', \ldots X^{(n-2)} \equiv 0 \ (mod\ p),$$

die den ersten Grad übersteigen, Genüge leisten, und dass dieses mit Nothwendigkeit eintrete, kann nicht behauptet werden. Vielmehr kann man ebenso, wie es Gleichungen höherer Grade mit nur imaginären Wurzeln giebt, auch eine Menge von solchen Formen der Grösse X angeben, welche niemals für irgend welche reelle Zahlenwerthe von x der Null congruent werden. — Dasselbe, was von der Congruenz

$$X \equiv 0 \ (mod\ p)$$

gilt, kann sogleich auf die Congruenz

$$X \equiv b \ (mod\ p)$$

übertragen werden; denn die letztere Form geht sogleich in die erstere über, sobald man auf beiden Seiten, wie es statthaft ist, die Grösse b subtrahirt.

Wenn es nun wirklich n von einander verschiedene Zahlen $a', a'', a''', \ldots a^{(n)}$ giebt, durch welche $X \equiv 0$ gemacht wird, so folgt, ähnlich wie bei den Gleichungen

$$X = mx^n + m'x^{n-1} + m''x^{n-2} + \ldots + m^{(n-1)}x + m^{(n)}$$
$$= m(x - a')(x - a'')(x - a''') \ldots\ldots (x - a^{(n)})$$

und, da wir für $a', a'', a''', \ldots$ beliebige unter den unzählig vielen Zahlen, die ihnen nach dem Modul p congruent sind, nehmen können, so muss es eine unendliche Menge von solchen Entwickelungen X geben, welche in Bezug auf den numerischen Werth des Coefficienten von x zwar verschieden sind, aber doch durch dieselben Congruenzen befriedigt werden; zwei algebraische Ausdrücke X von ganz verschiedener Form können mithin zu dem Modul p das nämliche Verhalten haben, d. h. dieselben Congruenzen

nach diesem Modul ausdrücken. Man nennt solche Ausdrücke **identische** Ausdrücke. Uebrigens können dieselben immer durch Multiplication mit einem passenden Factor und darauf erfolgende Abwerfung der Vielfachen von p, sodass nur die keinsten Reste der Coefficienten von x nach diesem Modul übrig bleiben, auf dieselbe Urform zurückgebracht werden.

Sei z. B. die Congruenz

$$2x^2+3x+5 \equiv 0 \; (mod\; 19)$$

aufzulösen. Setzen wir den Ausdruck zunächst geradezu der 0 gleich und lösen die entstehende Gleichung algebraisch auf, so folgen für x die beiden Wurzelwerthe

$$x = \frac{-3+\sqrt{-31}}{4},\; \frac{-3-\sqrt{-31}}{4}$$

und mithin

$$x^2+\frac{3}{2}x+\frac{5}{2}=\left(x-\frac{-3+\sqrt{-31}}{4}\right)\left(x-\frac{-3+\sqrt{-31}}{4}\right)$$

oder, wenn wir zur Beseitigung der Brüche mit 16 auf beiden Seiten multipliciren,

$$16x^2+24x+40=(4x+3-\sqrt{-31})(4x+3+\sqrt{-31}).$$

Dies führt uns darauf, dass wir die vorgelegte Congruenz mit 8 multipliciren, wodurch ja nichts geändert wird. Dies giebt uns

$$16x^2+24x+40 \equiv 0$$

oder auch

$$(4x+3)^2 \equiv -31$$

oder endlich, wenn wir den kleinsten Rest nehmen

$$(4x+3)^2 \equiv 7 \; (mod\; 19).$$

Die Auflösung unserer Congruenz ist jetzt auf die Frage zurückgeführt, ob es möglich ist für x eine solche ganze Zahl zu finden, dass $(4x+3)^2$ den Rest 7 lasse oder umgekehrt, ob es ein Vielfaches von 19 giebt, welches um 7 vergrössert ein vollständiges Quadrat wird. Wir können diese Frage vorläufig nur durch Probiren entscheiden und sehen leicht, dass

$$(4x+3)^2 \equiv 7+3.19 \; (mod\; 19)$$

ist. Dieser Congruenz wird offenbar durch zwei Annahmen gleichmässig Genüge geleistet, nämlich entweder durch die Annahme

$$4x+3 \equiv +8$$

oder durch die Annahme

$$4x+3 \equiv -8$$

und aus diesen Annahmen folgt

$$x \equiv 6 \text{ oder } 2 \ (mod\ 19)$$

und dieses sind mithin die beiden Lösungen der gegebenen Congruenz. In der That kann man dieselbe wieder rückwärts daraus erhalten. Nämlich durch die Multiplication folgt

$$(x-6)(x-2) = x^2-8x+12 \equiv 0 \ (mod\ 19)$$

und diese Form ist der gegebenen Form

$$2x^2+3x+5$$

offenbar identisch, wie man sogleich erkennt, wenn man sie mit 2 multiplicirt und dann überall statt der sich ergebenden Coefficienten deren kleinste Reste einführt.

In dem vorliegenden Falle haben wir die Auflösung durch einfaches Probiren gefunden, indem es uns glückte eine vollständige Quadratzahl 64 aufzufinden, welche durch 19 dividirt den Rest 7 lässt. Man sieht aber leicht ein, dass es in vielen Fällen nicht gelingen wird eine solche Quadratzahl aufzutreiben, welche durch eine einzelne Zahl dividirt einen gegebenen Rest lässt. Man unterscheidet daher, um gleich vorläufig diese Benennung zu erwähnen, solche Zahlen, welche für einen gewissen Modul als Rest bleiben können, durch den Namen quadratischer Reste (quadratica residua) von solchen, die in Bezug auf denselben Modul als Reste überhaupt nicht bleiben können, den quadratischen Nichtresten (quadratica non residua). So z. B. ist 7 ein quadratischer Rest von 19. Dagegen ist 2 ein quadratischer Nichtrest in Bezug auf den Modul 3. Denn es existirt keine Quadratzahl, welche durch 3 dividirt 2 zum Reste haben könne. Um dieses einzusehen, bemerke man, dass alle ganzen Zahlen in Bezug auf den Modul 3 nur eine der Formen

$$3n,\ 3n+1,\ 3n+2$$

haben können; hieraus entspringen für die Reihe der Quadratzahlen die Formen

$$9n^2,\ 9n^2+6n+1,\ 9n^2+12n+4,$$

denen nach dem Modul 3 die Reste

$$0,\ 1,\ 1$$

entsprechen, so dass 2 überhaupt nicht vorkommen kann.

Betrachten wir allgemeiner die Congruenz

$$ax^2+2bx+c \equiv 0 \ (mod\ p)$$

und bringen sie auf die Form

$$a^2x^2+2abx+b^2-(b^2-ac)\equiv 0,$$

so folgt

$$(ax+b)^2\equiv b^2-ac \pmod p$$

und es muss mithin zugesehen werden, ob b^2-ac ein quadratischer Rest zu dem Modul p ist oder ein Nichtrest. Im ersteren Falle sei q^2 die, etwa durch Versuche bestimmte, Quadratzahl, für welche b^2-ac als Rest bleibt; dann sind noch die beiden Congruenzen vom ersten Grade

$$\left.\begin{array}{l} ax+b\equiv +q \\ ax+b\equiv -q \end{array}\right\} \pmod p,$$

welche beide der gegebenen Congruenz Genüge leisten, aufzulösen.

Sei ferner die Congruenz

$$(ax-b)^3-c\equiv 0 \pmod p$$

aufzulösen, so kommt dies wieder auf die Untersuchung hinaus, ob eine reine Cubikzahl existire, welche nach dem Modul p den Rest c lässt. Ist eine solche Zahl q^3 ausfindig gemacht, so hat man

$$(ax-b)^3\equiv c\equiv q^3 \pmod p$$

und dieser Congruenz geschieht offenbar Genüge durch die Congruenz des ersten Grades

$$ax-b\equiv q \pmod p.$$

Die Untersuchung der übrigen Wurzeln geht in Uebereinstimmung mit dem Gange vor sich, den wir oben beim Beweise des vorausgeschickten Satzes angedeutet haben. Indem man nämlich die Congruenz

$$q^3\equiv c \pmod p$$

von der gegebenen abzieht, folgt

$$(ax-b)^3-q^3\equiv 0 \pmod p$$

oder auch

$$(ax-b-q)\,[(ax-b)^2+q(ax-b)+q^2]\equiv 0;$$

mithin, wenn noch Wurzeln ausser der schon gefundenen existiren, so ist dieses nur so möglich, dass dieselben zu gleicher Zeit der Congruenz vom zweiten Grade

$$(ax-b)^2+q(ax-b)+q^2\equiv 0 \pmod p$$

angehören, welcher wir auch die für die Untersuchung geeignetere Form

$$\{2(ax-b)+q\}^2\equiv -3q^2 \pmod p$$

geben können.

Untersuchen wir z. B. die Congruenz

$$3x^3 \equiv 4 \pmod{11}$$

und geben ihr zunächst die passendere Form

$$(3x)^3 \equiv 36 \equiv 3 \pmod{11},$$

so findet man unmittelbar, dass 3 ein kubischer Rest ist; denn

$$9^3 = 729 \equiv 3 \pmod{11};$$

mithin hat man

$$(3x)^3 - 9^3 \equiv 0 \pmod{11}$$

oder

$$(3x-9)(9x^2+27x+81) \equiv 0 \pmod{11}.$$

Eine Wurzel unserer Congruenz ist jetzt $3x-9 \equiv 0$ oder einfacher

$$x \equiv 3 \pmod{11}$$

und wenn noch andere vorhanden sind, so gehören dieselben zu gleich Zeit der Congruenz

$$9x^2+27x+81 \equiv 0 \pmod{11}$$

vom zweiten Grade an. Diese letztere mit 4 multiplicirt lässt sich, w folgt, schreiben:

$$(6x+9)^2 \equiv -243 \equiv 10 \pmod{11}.$$

Nun existirt aber keine Quadratzahl, die durch 11 dividirt den Rest lassen könnte. Denn alle Quadratzahlen stehen nothwendig unter einer d 11 Formen

$$(11n)^2,\ (11n+1)^2,\ (11n+2)^2,\ (11n+3)^2,\ \ldots..\ (11n+10)^2,$$

denen der Reihe nach die Reste

$$0,\ 1,\ 4,\ 9,\ 5,\ 3,\ 3,\ 5,\ 9,\ 4,\ 1$$

entsprechen. Mithin ist der Rest 10 nicht möglich oder ein quadratisch Nichtrest; dem zu Folge ist auch unsere zuletzt betrachtete Congrue zweiten Grades unmöglich und unsere cubische Congruenz besitzt dem Folge nur eine einzige reelle Wurzel, nämlich $x \equiv 3$.

Ziehen wir aus den vorstehenden Beispielen das allgemeine Endr sultat, so geht daraus hervor, dass für die Auflösung der Congruenz höherer Grade von der äussersten Wichtigkeit die Betrachtung der Re ist, welche eine Potenz nach einem gegebenen Modul lassen kann. Di ist also der Gegenstand, zu dem wir naturgemäss übergehen, und w lassen daher im folgenden Paragraphen den berühmten Fermat'schen S folgen, welcher das Fundament für die Theorie der Potenzreste bildet.

§. 10.

Fermat's Lehrsatz.

1) Ist p eine Primzahl und x eine nicht durch p theilbare, aber sonst vollkommen willkürliche Zahl, so ist

$$x^{p-1} \equiv 1 \pmod p.$$

Der Beweis stützt sich auf den bekannten Satz, dass, wenn man die Glieder der folgenden Reihe

$$1x\ 2x\ 3x\ 4x \ldots\ldots (p-2)x\ (p-1)x$$

nach einander durch p dividirt, die Reste verschieden sind und zwar, abgesehen von der Reihenfolge, mit den Zahlen

$$1\ 2\ 3\ 4 \ldots\ldots (p-2)\ (p-1)$$

übereinkommen. Mithin muss nothwendig das Product sämmtlicher Glieder der ersten Zahlenreihe dem Producte sämmtlicher Glieder der zweiten Zahlenreihe nach dem Modul p congruent sein und wir erhalten dadurch, da die Zahl der Glieder gleich $p-1$ ist,

$$1.2.3.4 \ldots\ldots (p-2)\ (p-1)\, x^{p-1} \equiv 1.2.3.4 \ldots\ldots (p-2)\ (p-1) \pmod p.$$

Diese Congruenz kann aber, da $1.2.3 \ldots (p-1)$ und p zu einander relative Primzahlen sind, ohne ihre Geltung zu verlieren, durch die erstere der beiden eben genannten Zahlen dividirt werden und geht alsdann in die zu erweisende über:

$$x^{p-1} \equiv 1 \pmod p.$$

Beispiele. Sei $x = 3$, $p = 5$, so hat man nach dem Modul 5

$$1.3 \equiv 3,\ 2.3 \equiv 1,\ 3.3 \equiv 4,\ 4.3 \equiv 2$$

und durch Multiplication dieser Congruenzen

$$1.2.3.4.3^4 \equiv 3.1.4.2 \pmod 5,$$

also durch Division

$$3^4 \equiv 1 \pmod 5.$$

Es ist ferner aus ähnlichen Gründen, immer nach dem Modul 5,

$$2^4 = 16 \equiv 1,\ 4^4 = 256 \equiv 1,\ 6^4 = 1296 \equiv 1.$$

Der vorstehende Satz wird gewöhnlich nach seinem Erfinder Fermat genannt. Offenbar setzt er voraus, dass die Zahl x kein Vielfaches von p sein darf; denn dann wäre auch x^{p-1} ein Vielfaches des Moduls und nicht blos die $(p-1)$te, sondern jede beliebige Potenz von x wäre der 0 und nicht der 1 congruent. Dieses ist aber auch die einzige Beschränkung,

welche der Zahl x auferlegt ist. Was die Zahl p betrifft, so kann sie jede beliebige Primzahl sein: dagegen ist der Satz nicht mit Nothwendigkeit gültig, wenn der Modul p eine zusammengesetzte Zahl ist. In diesem Falle nämlich ist die Division der durch die Multiplication im Beweise sich ergebenden Congruenz durch $1.2.3\ldots(p-1)$ nicht gerechtfertigt, weil der genannte Divisor keine relative Primzahl zu dem Modul ist. Ausserdem würde dann, damit schon der vorhergehende Theil des Beweises seine Gültigkeit nicht einbüsse, die Grösse x noch der weiteren Beschränkung unterworfen werden müssen, dass sie nur als relative Primzahl zu p angenommen werden darf. Wir wollen jetzt die Modification näher betrachten, welche für einen zusammengesetzten Modul in der Aussprache des Satzes sich herbeiführen.

2) Sei also p eine zusammengesetzte Zahl und die Zahlen, welche kleiner als p und relative Primzahlen zu p sind, dargestellt durch die Zahlenreihe

$$1\ m'\ m''\ m'''\ \ldots\ldots\ p-1;$$

wenn alsdann x eine relative Primzahl zu p bezeichnet, so haben die Vielfachen

$$1x\ m'x\ m''x\ m'''x\ \ldots\ldots\ (p-1)x$$

nach dem Modul p lauter von einander verschiedene Reste, welche relative Primzahlen zu p sind. Dass sie verschieden sind, folgt aus dem allgemeineren Satze, welchen wir der Theorie der Congruenz ersten Grades vorausschickten; wir haben also nur noch zu erweisen, dass sie alle relative Primzahlen zu p sind. Wäre dies nicht der Fall und etwa irgend ein solches

$$mx = ap + \alpha,$$

so dass α einen Theiler mit p gemeinschaftlich hätte, so müsste auch die linke Seite dieser Gleichung durch den nämlichen Theiler dividirbar sein, mithin entweder m oder x, so dass auf jeden Fall entweder m und p oder x und p einen gemeinsamen Divisor besässen, im Widerspruche zu der Voraussetzung, nach der sie relative Primzahlen sind. Da also alle Reste, welche bei der Division der einzelnen Glieder der Reihe

$$1x\ m'x\ m''x\ m'''x\ \ldots\ (p-1)x$$

durch den Modul p bleiben können, verschieden sind, da sie alle relative Primzahlen zu p und kleiner als p sind, da endlich die Anzahl dieser

Reste der Anzahl der relativen Primzahlen, die kleiner als p sind, gleich ist: so können sie nur mit der Reihe der relativen Primzahlen selbst zusammenfallen uud sind also, immer abgesehen von der Ordnung, gleich der Reihe der Zahlen

$$1\ m'\ m''\ m''' \ldots.\ p-1.$$

Man schliesst nun ganz in derselben Weise, wie vorhin, weiter. Es muss das Product sämmtlicher Glieder der vorletzten Reihe dem Producte sämmtlicher Glieder der letzten congruent sein, also da die Anzahl dieser Glieder das ist, was wir in der Einleitung als $S'''p$ bezeichneten,

$$1.m'.m''.m''' \ldots..(p-1)x^{S'''p} \equiv 1.m'.m''.m''' \ldots..(p-1)\ (mod\ p);$$

diese Congruenz kann durch $1.m'.m''.m''' \ldots.(p-1)$ dividirt werden, denn dieses Product ist relative Primzahl zu p, weil es die einzelnen Factoren sind, und man erhält dadurch

$$x^{S'''p} \equiv 1\ (mod\ p).$$

Für den Fall, dass p eine absolute Primzahl ist, wird

$$S'''p = p-1$$

und wir kommen mithin auf den vorigen Satz zurück. Dies giebt den Beweis, dass der jetzt gewonnene Satz das verallgemeinerte Fermat'sche Theorem ist und wir sprechen dasselbe jetzt, wie folgt, aus:

Wenn x eine willkürliche relative Primzahl zu dem Modul p und

$$n = S'''p$$

die Anzahl aller relativen Primzahlen bezeichnet, die kleiner als p sind, so findet immer die Congruenz statt:

$$x^n \equiv 1\ (mod\ p).$$

Beispiele. Die relativen Primzahlen zu 24, welche kleiner als 24, sind 1 5 7 11 13 17 19 23, mithin

$$S'''24 = 8.$$

Bilden wir uns nun die Producte einer beliebigen zu 24 relativen Primzahl, etwa 31, in die eben erwähnten Zahlen, so bekommen wir die folgenden auf den Modul 24 sich beziehenden Congruenzen

$$\left.\begin{array}{rlrl} 1.31 \equiv & 7, & 13.31 \equiv & -\ 5 \text{ oder } 19 \\ 5.31 \equiv & 11, & 17.19 \equiv & -\ 1 \text{ oder } 23 \\ 7.31 \equiv & 1, & 19.31 \equiv & -11 \text{ oder } 13 \\ 11.31 \equiv & 5, & 23.31 \equiv & -\ 7 \text{ oder } 17 \end{array}\right\}\ (mod\ 24)$$

und die Multiplication aller dieser Congruenzen giebt

$$1.5.7.11.13.17.19.23.31^8 \equiv 7.11.1.5.19.23.13.17,$$

woher

$$31^8 \equiv 1 \ (mod\ 24).$$

Macht man die Probe direct, so findet man

$$31 \equiv 7,\ 31^2 \equiv 7^2 \equiv 1,$$

und mithin durch Erhebung der letztgefundenen Congruenz auf die 4te Potenz die gesuchte Congruenz.

Sei ferner $p = 18$, so sind die relativen Primzahlen dazu, welche die Zahl 18 nicht übersteigen, der Reihe nach

1 5 7 11 13 17

also

$$S'''p = 6$$

und es folgt, wenn man $x = 25$ setzt,

$$25^6 \equiv 1 \ (mod\ 18);$$

in der That findet man

$$25 \equiv 7,\ 25^2 \equiv 7^2 \equiv -5,\ 25^3 \equiv -5.7 \equiv +1,$$

und die letzte Congruenz giebt durch Quadrirung die gesuchte.

Es ist nicht unzweckmässig auch ein Beispiel zu geben für den Fall, in welchem der Satz von Fermat keine Anwendung findet, nämlich wenn p ein zusammengesetzter Modul und x keine relative Primzahl dazu ist. Sei also

$$p = 15,\ x = 18.$$

Die Reihe der relativen Primzahlen zu p kleiner als diese Zahl wird alsdann

1 2 4 7 8 11 13 14

und wir können uns nun folgende beiden Reihen bilden, in deren ersterer die Vielfachen von 18 verzeichnet sind, während in der letzten jedes Mal unter dem bezüglichen Vielfachen der zugehörige Rest steht, welchem es congruent ist:

1.18	2.18	4.18	7.18	8.18	11.18	13.18	14.18
+3	+6	−3	+6	−6	+3	−6	−3
		od. +12		od. +9		od. +9	od. +12

Man sieht hieraus, dass die Reste durchaus nicht verschieden ausfallen, sondern jeder wiederholt sich zweimal und man bekommt daher, wenn man multiplicirt und bei der Multiplication an Stelle der Zahlen 8, 11, 13, 14 die kleinsten Reste −7, −4, −2, −1 setzt

$$(1.2.4.7)^2.18^8 \equiv (3.6)^4 \ (mod\ 15)$$

oder wenn man statt 18 und 3 . 6 gleichfalls den Rest 3 substituirt

$$(1 . 2 . 4 . 7)^2 . 3^8 \equiv 3^4 \ (mod\ 15).$$

Die Congruenz 18^8 oder $3^8 \equiv 1$ lässt sich hieraus auf keine Weise ableiten und wäre auch falsch: denn man findet allmählig:

$$\begin{array}{ll} 18^1 \equiv 3 & 18^5 \equiv +3 \\ 18^2 \equiv -6 \equiv 9 & 18^6 \equiv -6 \equiv +9 \\ 18^3 \equiv -3 \equiv 12 & 18^7 \equiv -3 \equiv +12 \\ 18^4 \equiv +6 & 18^8 \equiv +6 \end{array} \quad (mod\ 15)$$

Man sieht leicht, dass, wie weit man auch fortgehen möge, diese viergliedrige Periode der Reste, nämlich

$$+3, \ -6, \ -3, \ +6,$$

sich immer und immer wiederholen wird, so dass der Rest 1 nach dem Modul 15 überhaupt für keinen Werth des Exponenten möglich ist.

3) Schon aus dem vorhergehenden Beispiel kann man mit Leichtigkeit abnehmen, dass eine Potenz, deren Exponent $S'''p$ und deren Grundzahl irgend eine zu p relative Primzahl x ist, wohl immer der Congruenz 1 genügt, aber im Allgemeinen weder die einzige, noch auch die niedrigste Potenz sein wird, für welche dasselbe eintritt. Sie ist die einzige schon darum keineswegs, weil, indem man die Gleichung

$$n^{S'''p} \equiv 1 \ (mod\ p)$$

auf die *m*te Potenz erhebt, sich sogleich

$$2^{mS'''p} \equiv 1 \ (mod\ p)$$

ergiebt und mithin alle solche Potenzen, deren Exponenten Vielfache von $S'''p$ sind, gleichfalls 1 werden. Sie ist aber im Allgemeinen auch nicht die niedrigste; vielmehr können thatsächlich viele Fälle aufgezeigt werden, in denen niedrigere Exponenten als $S'''p$ die Congruenz 1 gleich wohl erfüllen. Ein Exponent muss aber selbstverständlich in allen Fällen existiren, welcher der niedrigste ist, so dass jede Potenz mit noch niedrigerem Exponenten von der 1 verschieden ausfällt. Sei dieser Exponent q, so ist

$$x^q \equiv 1 \ (mod\ p)$$

und man sagt alsdann: die Grundzahl x gehört zu dem Exponenten q. Von einem solchen Exponenten gilt nun folgender Satz:

Ist q eine positive Zahl von der Beschaffenheit, dass die $q$te Potenz von x die niedrigste ist, welche der Einheit gleich wird, d. h. wenn x zu dem Exponenten q gehört; so

ist q ein Divisor von dem Exponenten einer jeden Potenz von a, welche in Bezug auf denselben Modul p sich auf die Einheit reducirt.

Sei also für einen beliebigen Exponenten r, der grösser als q ist,

$$x^r \equiv 1 \,(mod\, p)$$

und wäre gleichzeitig

$$r = sq + t, \; t < q,$$

so würde, wenn man in der vorhergehenden Congruenz für r diesen Werth substituirt, folgen

$$x^{sq+t} = x^{sq} x^t \equiv 1 \; (mod\, p)$$

und hieraus, da

$$(x^q)^s = x^{sq} \equiv 1 \; (mod\, p),$$

wenn man für x^{sq} seinen kleinsten Rest 1 setzt,

$$x^t \equiv 1 \; (mod\, p).$$

Nun ist aber t der Rest, welcher bei der Division von r durch q bleiben soll, also ist $t < q$ und es existirt also eine niedrigere Potenz als die niedrigste, welche gleich 1 wird. Dieser Widerspruch bleibt, so lange man t von 0 verschieden annimmt; man ist mithin genöthigt r als ein Vielfaches von q anzunehmen.

Wenn also verschiedene Zahlen, als Exponenten zu irgend einer Grundzahl gesetzt, diese nach irgend einem Modul der Einheit congruent machen, so ist die kleinste unter ihnen ein Factor der übrigen. Ist daher p speciell eine Primzahl, so muss die kleinste Zahl q ein Factor von $p-1$ sein; dies schliesst aber durchaus nicht den Fall aus, dass nicht mitunter q mit $p-1$ zusammenfallen könne.

Weiter gehört hierher noch folgender Satz:

Wenn die Zahl x zu dem Exponenten q gehört, so sind die Reste der Potenzen

$$1 \quad x \quad x^2 \quad x^3 \quad x^4 \; \ldots\ldots \; x^{q-1}$$

in Bezug auf den Modul p alle von einander verschieden.

Denn existirten zwei, die einander congruent wären, etwa

$$x^m \equiv x^n \,(mod\, p)$$

und wäre $m > n$, so folgte

$$x^n (x^{m-n} - 1) \equiv 0 \; (mod\, p).$$

Nun ist aber, der Voraussetzung zu Folge, x eine relative Primzahl zu p, also weder x noch irgend eine Potenz von x durch p ohne Rest theilbar:

mithin kann die vorstehende Congruenz nicht anders befriedigt werden, als indem man

$$x^{m-n} - 1 \equiv 0 \ (mod\, p),$$

also

$$x^{m-n} \equiv 1 \ (mod\, p)$$

annimmt. Das ist aber ein offenkundiger Widerspruch. Denn m und n sind schon an sich kleinere Zahlen als q; mithin ist es $m-n$ noch viel stärker und es existirte sonach eine Zahl $m-n$ kleiner als die kleinste q, für welche die bezügliche Potenz der Einheit congruent würde.

Zu den zuletzt angeführten Sätzen mögen folgende Beispiele hinzugefügt werden.

$$mod = p = 19, \ S'''p = 18$$

24 gehört zu	24^0	24^1	24^2	24^3	24^4	24^5	24^6	24^7	24^8
$q=9$	1	5	6	-8	-2	9	7	-3	4

15 gehört zu	15^0	15^1	15^2	15^3	15^4	15^5	15^6	15^7	15^8	15^9	15^{10}	15^{11}	15^{12}	15^{13}	15^{14}	15^{15}	15^{16}	15^{17}
$q=18$	1	-4	-3	-7	9	2	-8	-6	5	-1	4	3	7	-9	-2	8	6	-5

$$mod = p = 36, \ S'''p = 12$$

5 gehört zu	5^0	5^1	5^2	5^3	5^4	5^5
$q=6$	1	5	-11	17	13	-7

25 gehört zu	25^0	25^1	25^2	125 gehört zu	125^0	125^1
$q=3$	1	-11	13	$q=2$	1	17

7 gehört zu	7^0	7^1	7^2	7^3	7^4	7^5	11 gehört zu	11^0	11^1	11^2	11^3	11^4	11^5
$q=6$	1	7	13	-17	-18	-5	$q=6$	1	11	13	-1	-11	-13

Die vorhergehende Progression, welche nach der Grösse x fortschreitet, gestattet noch eine interessante Bemerkung. Bilden wir uns die Summe ihrer Glieder, so ist immer

$$1 + x + x^2 + x^3 + \ldots. + x^{q-1} \equiv 0 \ (mod\, p).$$

Zum Beweise gehen wir von der identischen Gleichung

$$(1 + x + x^2 + x^3 + \ldots. + x^{q-1})(x-1) = x^q - 1$$

aus und folgern hieraus, da

$$x^q - 1 \equiv 0 \ (mod\, p)$$

sogleich die neue Congruenz

$$(1 + x + x^2 + \ldots. + x^{q-1})(x-1) \equiv 0 \ (mod\, p).$$

Nun kann $x-1$ nicht der Null congruent werden, wenigstens sobald wir x von 1 verschieden annehmen, und es kann mithin die vorstehende Congruenz nicht anders erfüllt werden, als indem man die behauptete setzt. Was aber den bezeichneten Ausnahmefall betrifft, so ist derselbe auch nur scheinbar vorhanden. Denn wenn man

$$x = 1,\ p+1,\ 2p+1,\ \ldots.$$

hat, so ist schon die erste Potenz von x der Einheit congruent, also $q = 1$, und die Progression reducirt sich auf ihr erstes Glied 1.

Was das Product dieser verschiedenen Potenzen betrifft, so hat man davon einen ähnlichen Satz. Es ist nämlich

$$1 \,.\, x \,.\, x^2 \,.\, x^3 \,.\, x^4 \,.\, x^5 \ldots\ldots x^{q-1}$$

im Falle eines ungeraden q $\equiv +1$,

und im Falle eines geraden q $\equiv -1$;

indessen müssen wir den Beweis für diese Behauptung vorläufig noch aufsparen, weil derselbe eines Satzes bedarf, der erst weiter unten bewiesen werden kann.

§. 11.

Von den Zahlen, welche zu einem gegebenen Exponenten gehören.

1) Nehmen wir im Nachfolgenden wieder p als absolute Primzahl an, so wissen wir aus den vorhergehenden Untersuchungen, dass nur Divisoren von $p-1$ zu Exponenten solcher Potenzen von x gemacht werden können, welche gleich 1 sind und zugleich die niedrigsten, welche diese Eigenschaft besitzen. Naturgemäss drängt sich die Frage auf, wenn q irgend ein Theiler von $p-1$ ist, giebt es dann immer wenigstens eine Zahl x, welche zu dem Exponenten q gehört, d. h. einer der Einheit congruenten Potenz entspricht, welche die niedrigste ist, und wenn solche Zahlen existiren, wie viele giebt es, die nach dem Modul p von einander verschieden sind. Den ersten Theil dieser Fragestellung wollen wir dadurch erledigen, dass wir zunächst q geradezu als einen Primfactor von $p-1$ annehmen, darauf als die Potenz irgend eines Primfactors, endlich als eine aus den verschiedenen Primfactoren von $p-1$ sich beliebig zusammensetzende Zahl. Das Resultat der Untersuchung spricht sich in folgendem Theoreme aus:

Es giebt immer eine Zahl Q, welche zu einem gegebenen Divisor q von $p-1$ gehört, wie dieser Divisor auch immer aus den Primfactoren von $p-1$ sich zusammensetzen möge.

Sei also zuerst q ein Primfactor von $p-1$, so wird

$$p-1 = qq'$$

gesetzt werden können und die Congruenz

$$x^{q'} \equiv 1 \pmod p$$

kann höchstens q' von einander verschiedene Lösungen haben. Indem wir daher die Glieder der Zahlenreihe

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \ldots\ldots p-1$$

nacheinander für x einsetzen, können höchstens q' derselben jene Congruenz befriedigen und es bleiben daher mindestens $p-1-q'$ Glieder übrig, für welche $x^{q'}$ einen von der Einheit verschiedenen Rest hat. Dies Raisonnement wird bloss für q' gleich $p-1$ ungültig, weil dann möglicher Weise kein Glied übrig bleibt; aber für diesen Fall haben wir auch gar nicht nöthig die Möglichkeit der Congruenz

$$x^{\frac{p-1}{q}} = x^{p-1} = x \equiv 1 \pmod p$$

nachzuweisen, da sie alsdann eine Congruenz ersten Grades und durch den Werth 1 der Unbestimmten x erfüllt wird. In allen anderen Fällen dagegen ist $p-1-q'$ eine ganz positive Zahl, die grösser als 1 ausfällt und es bleiben daher immer mehrere Glieder übrig, für welche die bezügliche Potenz von 1 verschieden wird. Nehmen wir mithin für x ein solches Glied, so wird nothwendig

$$x^{q'} = x^{\frac{p-1}{q}} \equiv h \pmod p$$

und h hierbei von 1 sich verschieden ergeben. Indem wir diese Congruenz auf die Potenz q erheben, folgt

$$x^{p-1} \equiv h^q \pmod p$$

oder, da x^{p-1} nach dem Fundamentaltheoreme von Fermat gleich 1 ist,

$$h^q \equiv 1 \pmod p.$$

Wenn nun aber h zu dem Exponenten q wirklich gehören soll, ist es nicht genug, dass h^q der Einheit gleich wird, sondern es muss auch h^q die niedrigste Potenz von h sein, welche der Einheit gleich wird. Wäre aber nicht h^q, sondern h^δ die niedrigste Potenz, für welche

$$h^\delta \equiv 1 \pmod p,$$

so folgte nach Nr. 3) des vorigen Paragraphen, dass δ ein Factor von q wäre. Dies ist aber, da q als eine Primzahl angenommen ist, nicht anders möglich, als wenn δ entweder gleich 1 oder gleich q ist. Die Annahme $\delta = 1$ ist widersprechend, weil h verschieden von 1 bestimmt ist, also

bleibt nur die zweite Annahme $\delta = q$ übrig, in welcher gerade das l was wir beweisen wollen. —

Sei ferner, indem a einen Primfactor von $p-1$ bezeichnet,

$$q = a^\alpha,$$

so ist zunächst wieder der Nachweis zu führen, dass wenigstens eine ; h existirt, welche der Congruenz

$$h^{a^\alpha} \equiv 1 \pmod p$$

genügt. Nun lässt sich aber, wie vorhin bewiesen ist, unter den Zahle

$$1 \quad 2 \quad 3 \quad 4 \ldots\ldots p-1$$

immer eine Zahl g von der Beschaffenheit finden, dass die Congruenz

$$g^{\frac{p-1}{a}} \equiv h' \pmod p$$

befriedigt wird, wo h' von 1 verschieden ausfällt. Ist nun $g^{\frac{p-1}{a}}$ von 1 v schieden, so muss es auch $g^{\frac{p-1}{a^\alpha}}$ sein. Denn wäre

$$g^{\frac{p-1}{a^\alpha}} \equiv 1 \pmod p,$$

so folgte durch Erhebung auf die Potenz $a^{\alpha-1}$

$$g^{\frac{p-1}{a}} \equiv 1^{a^{\alpha-1}} = 1 \pmod p,$$

im Widerspruche damit, dass der Rest von $g^{\frac{p-1}{a}}$ von der Einheit ' schieden bestimmt ist. Demgemäss ist es erlaubt

$$g^{\frac{p-1}{a^\alpha}} \equiv h \pmod p$$

zu setzen und hierbei h als eine von 1 verschiedene Zahl zu betrach Daraus folgt aber weiter durch Erhebung auf die Potenz a^α, wenn ı berücksichtigt, dass links $g^{p-1} \equiv 1$ kommt:

$$h^{a^\alpha} \equiv 1 \pmod p$$

und eine Zahl h, welche dieser Congruenz genügt, kann also unter ; Umständen ermittelt werden.

Zweitens ist darzuthun, dass keine niedrigere Potenz von h als a^αte der Einheit gleich werden kann. Wäre dies möglich und die niedri Potenz von h, welche der Einheit gleich wäre, etwa h^δ, so muss δ nothw dig ein Factor von a^α sein, also von der Form

$$\delta = a^\varrho, \ \varrho < \alpha.$$

Nun hat man wegen der Congruenz

$$g^{\frac{p-1}{a^\alpha}} \equiv h$$

durch Erhebung auf die Potenz $a^{\alpha-1}$

$$g^{\frac{p-1}{a}} \equiv h^{a^{\alpha-1}} \pmod p$$

und hieraus zwischen h und h' die Relation

$$h' \equiv h^{a^{\alpha-1}} \pmod p,$$

oder

$$h' \equiv h^{a^{\alpha-\varrho+\varrho-1}} = h^{a^\varrho \cdot a^{\alpha-1-\varrho}} = (h^{a^\varrho})^{a^{\alpha-1-\varrho}};$$

mithin, da der Annahme gemäss

$$h^{a^\varrho} \equiv 1$$

sein soll, müsste man haben $h' \equiv 1 \pmod p$, welches im Widerspruche mit der Art sich befindet, wie wir h' bestimmt haben.

Beispiel. Sei $p = 17$, also $p-1 = 16$, $a = 2$, $\frac{p-1}{a} = 8$. Alsdann hat man die 8ten Potenzen aller Zahlen von $1-16$ zu untersuchen, um diejenigen aufzufinden, welche von 1 verschieden sind. Die Resultate sind in den nachfolgenden beiden Reihen verzeichnet, in deren zweiter unter jeder Potenz der bezügliche Rest sich vorfindet:

1^8	2^8	3^8	4^8	5^8	6^8	7^8	8^8	9^8	10^8	11^8	12^8	13^8	14^8	15^8	16^8
1	1	-1	1	-1	-1	-1	1	1	-1	-1	-1	1	-1	1	1

Es sind also 8 Zahlen, nämlich

$$g = 3 \quad 5 \quad 6 \quad 7 \quad 10 \quad 11 \quad 12 \quad 14,$$

für welche die betrachtete Potenz von 1 verschieden ausfällt, nämlich gleich -1 oder $+16$ wird.

Suchen wir nun die Zahlen h, welche zu dem Exponenten

$$a^\alpha = 2^1 \equiv 2$$

gehören, so haben wir, da sich dieselben durch die Congruenz

$$g^{\frac{p-1}{a^\alpha}} \equiv h \pmod p$$

bestimmen, den Resten der Potenz $g^{\frac{16}{2}} = g^8$ zu untersuchen, welche sich für jene 8 verschiedenen Werthe von g ergiebt; aus der vorstehenden Entwickelung ergiebt sich, dass er jedesmal gleich 16 wird und mithin ist 16 die einzige Zahl, welche zu dem Exponenten 2 gehört.

In Betreff der Zahlen, welche zu dem Exponenten

$$a^\alpha = 2^2 = 4$$

gehören, ist die bestimmende Congruenz (da $\frac{p-1}{a^\alpha} = 4$)

$$g^4 \equiv h \pmod{p}$$

und die Substitution der 8 Werthe für g ergiebt nach der Reihe die Reste

$$h = -4 \quad -4 \quad 4 \quad 4 \quad 4 \quad 4 \quad -4 \quad -4$$

und mithin gehören zwei von einander verschiedene Zahlen zu dem Exponenten 4, nämlich

$$h = 4,\ 13.$$

Ferner, wenn der Exponent

$$a^\alpha = 2^3 = 8$$

untersucht wird, so findet man durch Substitution der 8 Werthe von g in die Bestimmungscongruenz

$$g^2 \equiv h \pmod{p}$$

nacheinander die Reste

$$h = -8 \ +8 \ +2 \ -2 \ -2 \ +2 \ +8 \ -8$$

und es gehören also zu dem Exponenten 8 die 4 verschiedenen Zahlen

$$h = 2,\ 8,\ 9,\ 15.$$

Endlich sei der Exponent

$$a^\alpha = 2^4 = 16,$$

so wird die Bestimmungscongruenz geradezu $g \equiv h$ und es gehören also zu unserem Exponenten 16 die 8 verschiedenen Werthe:

$$h = 3 \quad 5 \quad 6 \quad 7 \quad 10 \quad 11 \quad 12 \quad 14.$$

Der besseren Uebersicht halber wollen wir die Resultate der Entwickelung in folgender Tabelle zusammenstellen, wo links die betreffenden Divisoren von $p-1$ stehen und rechts daneben die zugehörigen Zahlen h:

1	1
2	16
4	4 13
8	2 8 9 15
16	3 5 6 7 10 11 12 14.

Man kann vorläufig schon aus der Betrachtung dieser Tabelle zu der Vermuthung kommen, dass die Anzahl der Zahlen, welche zu irgend einem Divisor gehören, gleich der Anzahl der relativen Primzahlen zu letzterem ist, welche kleiner als er sind, und in der That werden wir diesen Satz später beweisen. Uebrigens sieht man leicht, dass die Rechnung auf jeden Fall Abkürzungen gestatten muss, vermöge deren die Betrachtung solcher Potenzen von g, die dasselbe ergeben, überflüssig wird.

Nehmen wir jetzt ganz allgemein den Divisor q als ein aus den Primfactoren von $p-1$ sich beliebig zusammensetzendes Product an, also

$$q = a^\alpha . b^\beta . c^\gamma \ldots\ldots,$$

so suche man sich zunächst solche Zahlen zu bestimmen, nämlich

$$A, B, C \ldots\ldots,$$

welche zu den Divisoren

$$a^\alpha, b^\beta, c^\gamma \ldots\ldots$$

gehören, was, da wir $a, b, c, \ldots\ldots$ als Primzahlen annehmen, nach dem Vorigen immer geleistet werden kann; alsdann ist

$$A^{a^\alpha} \equiv 1, \quad B^{b^\beta} \equiv 1, \quad C^{c^\gamma} \equiv 1, \ldots\ldots (mod\ p),$$

also durch Erhebung dieser Congruenzen respective auf die $\frac{q}{a^\alpha}$te, $\frac{q}{b^\beta}$te, $\frac{q}{c^\gamma}$te, ... Potenz

$$A^q \equiv 1, B^q \equiv 1, C^q \equiv 1, \ldots\ldots$$

und hieraus durch Multiplication

$$(ABC\ldots\ldots)^q \equiv 1\ (mod\ p).$$

Es ist noch zu beweisen übrig, dass dies die niedrigste der Einheit gleiche Potenz von ABC ..... ist. Wäre $q > d$ und

$$(ABC\ldots\ldots)^d \equiv 1,$$

so dass jede kleinere Potenz von ABC .... von 1 verschieden ausfiele; so müsste q ein Vielfaches von d sein. Diese Zahl d kann man nun immer mit einer solchen Grösse x multipliciren, dass in dem Producte dx die Primzahlen $a, b, c, \ldots\ldots$ mit denselben Exponenten vorkommen, welche sie in $q = a^\alpha b^\beta c^\gamma \ldots\ldots$ haben, bis auf irgend eine Primzahl, etwa a, welche einen kleineren Exponenten α' als α bekommen soll, so dass

$$dx = a^{\alpha'} b^\beta c^\gamma \ldots\ldots$$

Dann kann man durch geeignete Potenzirung aus den Congruenzen

$$B^{b^\beta} \equiv 1, \quad C^{c^\gamma} \equiv 1, \ldots\ldots (mod\ p)$$

die folgenden herleiten

$$B^{dx} \equiv 1, \ C^{dx} \equiv 1, \ldots (mod\ p),$$

aus denen durch Multiplication sich

$$(BC\ldots\ldots)^{dx} \equiv 1$$

ergiebt. Ferner ist, weil $(ABC\ldots\ldots)^d \equiv 1$, auch

$$(ABC\ldots\ldots)^{dx} \equiv 1,$$

immer nach demselben Modul p. Dividirt man nun die letzte Congruenz

durch die vorhergehende, was zulässig ist, da $(BC\ldots)^{dx}$ und 1 zu dem Modul p relative Primzahlen sind, so folgt $A^{dx} \equiv 1$ oder

$$A^{a^{\alpha'} b^{\beta} c^{\gamma} \ldots} \equiv 1 \pmod p.$$

Da nun A zu dem Exponenten a^{α} gehört, so muss a^{α} ein Theiler von $a^{\alpha'} b^{\beta} c^{\gamma} \ldots$ sein, welches, da a, b, c, ... von einander verschiedene Primzahlen sind, nicht anders möglich ist, als wenn a^{α} ein Theiler von $a^{\alpha'}$ ist. Dieses ist aber ein Widerspruch, da α' kleiner als α ist. Mithin ist die Annahme falsch und alle Potenzen von $ABC\ldots$, welche niedriger sind, als die $q$te, von der Einheit verschieden, d. h. $ABC\ldots$ gehört zu dem Exponenten q.

2) Nachdem wir jetzt den Nachweis geliefert haben, dass immer wenigstens eine Zahl x existirt, welche zu einem gegebenen Divisor q von $p-1$ gehört, kommen wir an den anderen Theil unserer Untersuchung, wie viele solcher nach dem Modul p von einander verschiedene x existiren.

Um diese Frage zu erledigen, nehme man an, dass wir irgend eine Zahl h uns bestimmt haben, welche zu dem Exponenten q gehört, so folgt:

$$h^q \equiv 1 \pmod p$$

und wir bekommen, indem wir diese Congruenz nach einander auf die erste, zweite, dritte, ... $q$te Potenz erheben, die folgende Reihe von Congruenzen:

$$\left.\begin{array}{ll} h^q & \equiv 1 \\ (h^2)^q & \equiv 1 \\ (h^3)^q & \equiv 1 \\ \ldots\ldots & \\ \ldots\ldots & \\ (h^{q-1})^q & \equiv 1 \\ (h^q)^q & \equiv 1 \end{array}\right\} (mod\ b).$$

Weiter dürfen wir nicht gehen, weil wir sonst nur Wiederholungen des Früheren bekommen würden. Das nächste Glied z. B. würde

$$(h^{q+1})^q = (h^q)^q h^q = h^q \equiv 1,$$

und ähnlich steht es mit den folgenden. Es sind ferner die Grundzahlen der verschiedenen $q$ten Potenzen, die in unserer Congruenzenreihe vorkommen, nämlich

$$h,\ h^2,\ h^3,\ h^4,\ \ldots,\ h^{q-1},\ h^q$$

oder, wenn man für die letzte ihren Werth 1 setzt und sie dann voranstellt

$$1,\ h,\ h^2,\ h^3,\ \ldots\ldots\ h^{q-1}$$

nach dem Modul p alle von einander verschieden. Dies folgt, weil h zu dem Exponenten q gehört, nach einem Satze, der in der letzten Nummer des vorigen Paragraphen enthalten ist. Dieses alles zusammengefasst ist klar, dass die Zahlen der in der vorhergehenden Horizontalreihe zusammengestellten Potenzen von h die sämmtlichen Wurzeln der Congruenz

$$x^q \equiv 1 \ (mod\ p)$$

darstellen; denn einmal genügen sie sämmtlich, sobald sie für x substituirt werden, und dann sind sie von einander verschieden und der Anzahl nach so gross, wie die Anzahl q der Wurzeln, welche unsere Congruenz vom $q$ten Grade höchstens haben kann. Unter diesen Wurzeln müssen also auch diejenigen Zahlen sein, welche zu dem Exponenten q gehören. Es kommt nur darauf an sie aus der Menge der übrigen herauszuscheiden und ihre Anzahl zu bestimmen. Dieses geschieht nun mittelst des folgenden Theoremes:

Wenn r eine relative Primzahl zu q ist und die Zahl h zu dem Exponenten q gehört, so gehört auch die Zahl h^r zu dem Exponenten q.

Da h zu q gehört, so ist $h^q \equiv 1$ und mithin auch

$$(h^r)^q = h^{rq} \equiv 1 \ (mod\ p).$$

Wäre nun nicht die $q$te, sondern die q'te Potenz von h^r die kleinste, welche der Einheit gleich würde, so hätte man auch noch

$$(h^r)^{q'} = h^{rq'} \equiv 1 \ (mod\ p)$$

und da h zu q gehört, so müsste q ein Divisor von rq' sein; das geht, da der Voraussetzung nach r und q relative Primzahlen sind, nicht anders an, als wenn q ein Theiler von q': dies ist aber gleichfalls nicht statthaft, weil q' der Annahme nach kleiner als q sein muss. Also ist der Widerspruch nur so zu heben, dass man $q' = q$ annimmt.

Alle möglichen Zahlen, welche zu q gehören und nach dem Modul p von einander verschieden sind, müssen in der Reihe der obigen Potenzen von h enthalten sein, deren Exponenten sämmtlich kleiner als q sind, nämlich

$$0 \ 1 \ 2 \ 3 \ 4 \ldots\ldots q-1;$$

da nur allein diejenigen, welche relative Primzahlen zu q sind, brauchbar sind, so folgt ohne Weiteres das zweite Theorem, welches die Anzahl der zu einem Exponenten gehörigen Zahlen feststellt:

Die Anzahl der zu einem Exponenten q nach dem Modul p gehörigen Zahlen ist gleich der Anzahl aller Zahlen, die kleiner als dieser Exponent und relative Primzahlen zu q sind.

Die Rechnung, welche wir vorhin bei der Auffindung der zu irgend einem Exponenten gehörigen Zahlen angewandt haben, gestattet zu Folge der vorstehenden Entwickelungen bedeutende Abkürzungen. Es ergiebt sich nämlich jetzt hierfür folgende Regel:

Sei der betrachtete Divisor von $p-1$

$$q = a^\alpha b^\beta c^\gamma \ldots\ldots,$$

so bestimme man sich unter den Zahlen

$$1\ 2\ 3\ 4 \ldots\ldots\ldots p-1$$

die jedesmalige erste, für welche die den Exponenten

$$\frac{p-1}{a},\ \frac{p-1}{b},\ \frac{p-1}{c},\ \ldots\ldots$$

entsprechenden Potenzen von 1 verschieden ausfallen; es mögen diese Zahlen durch die Symbole

$$A',\ B',\ C',\ \ldots\ldots$$

bezeichnet werden. Hierauf suche man die Reste der Potenzen

$$A'^{\frac{p-1}{a^\alpha}},\ B'^{\frac{p-1}{b^\beta}},\ C'^{\frac{p-1}{c^\gamma}} \ldots\ldots;$$

es mögen dieselben in den kleinsten Zahlen ausgedrückt respective

$$A,\ B,\ C,\ \ldots\ldots$$

sein. Dann gehören $A,\ B,\ C, \ldots\ldots$ einzeln genommen zu den Exponenten $a^\alpha,\ b^\beta,\ c^\gamma \ldots\ldots$ und zu dem Exponenten q gehört das Product aller dieser Zahlen

$$Q = A.B.C\ldots\ldots$$

Nachdem dieses geschehen bestimme man sich sämmtliche Zahlen, welche relative Primzahlen zu q und kleiner als diese Zahl sind, nämlich

$$1\ q'\ q''\ q''' \ldots\ldots\ q-1;$$

so gehören zu dem Exponenten q die sämmtlichen Glieder der Zahlenreihe

$$Q,\ Q^{q'},\ Q^{q''},\ Q^{q'''},\ \ldots\ldots\ Q^{q-1}$$

und ausserdem keine anderen Zahlen, ausser etwa solchen, die nach dem Modul p mit einer der genannten übereinstimmen.

Man sieht leicht ein, dass auf diese Weise alles überflüssige Probiren beseitigt ist und nur bei Aufsuchung der Zahlen A', B', C, ... nöthig ist; alles andere ergiebt sich dann, wie q auch immer beschaffen sein möge, mit strenger Nothwendigkeit.

Beispiel. Nehmen wir

$$p = 73,\ p-1 = 72 = 2^3 . 3^2$$

an, so haben wir

$$\frac{p-1}{a} = 36,\ \frac{p-1}{b} = 24$$

und wenn man die Zahlen von 1 bis 72 untersucht, so findet man gleich im Anfange

$$\left.\begin{array}{l} 5^3 \equiv -21,\ 5^6 \equiv 3,\ 5^{12} \equiv 9,\ 5^{24} \equiv 8,\ 5^{36} \equiv 8.9 \equiv -1 \\ \qquad\qquad 2^3 \equiv 8,\ 2^6 \equiv 9,\ 2^{12} \equiv 8,\ 2^{24} \equiv 64 \equiv -9 \end{array}\right\} (mod\ 73)$$

und es folgt demgemäss

$$A' = 5,\ B' = 2.$$

Die verschiedenen Divisoren von $p-1$, welche wir der Reihe nach zu betrachten haben, sind

1 2 3 4 6 8 9 12 18 24 36 72.

Zu dem Divisor 1 gehört die einzige Zahl 1, in Uebereinstimmung damit, dass die einzige Zahl, welche relative Primzahl zu 1 und nicht grösser als sie ist, mit ihr selber zusammenfällt. Zu 2 kann auch nur eine einzige Zahl gehören, da blos eine relative Primzahl zu 2, die kleiner ist, existirt, nämlich 1. Dieselbe ist

$$A'^{\frac{p-1}{a}} = 5^{\frac{72}{2}} = 5^{36} \equiv -1 \text{ oder } 72.$$

Zu dem Divisor 3 gehört zunächst

$$B'^{\frac{p-1}{b}} = 2^{24} \equiv -9$$

und da die in Betracht kommenden relativen Primzahlen zu 3 1 und 2 sind, so gehören zu dem Exponenten 3 die Reste der beiden Poten ze

$$(-9)^1 \text{ und } (-9)^2,$$

nämlich

Zu dem Divisor 4 gehört

$$A'^{\frac{p-1}{a^2}} = 5^{18} \equiv 27,$$

mithin sind alle zugehörigen Zahlen die Reste der Potenzen 27^1 und 27^3, oder, was bequemer für die Rechnung ist, weil wir dann die zur Berechnung von 5^{36} benutzten Daten benutzen können, der Potenzen 5^{18} und $5^{54} = 5^{36} . 5^{12} . 5^6 \equiv -27$, mithin

$$27 \text{ und } 46.$$

Zu den Divisoren 6 gehört das Product irgend zweier Zahlen, die zu 2 und 3 gehören, also der Zahl 72 entweder mit 64 oder mit 8; dies giebt, wenn man die kleinsten Reste nimmt,

$$-1 . -9 \text{ und } -1 . +8$$

oder

$$9 \text{ und } 65.$$

Da zu 6 nur 2 Zahlen gehören können, nämlich 9^1 und 9^5 oder auch 65^1 und 65^5, so müssen die, welche durch Combination der zu 2 und 3 gehörigen Zahlen soeben gefunden wurden, mit diesen letzteren Potenzen zusammenfallen und in der That hat man

$$9^5 = 9 . (9^2)^2 \equiv 9 . 8^2 \equiv 9 . -9 \equiv -8 \equiv 65$$

und ebenso

$$65^5 \equiv (-8)^5 \equiv -8 . 64^2 \equiv -8 . (-9)^2 = -8 . 8 \equiv -64 \equiv 9.$$

Es ist überhaupt ganz im Allgemeinen klar, dass die Combination der den Exponenten a^α, b^β, c^γ, ... zugehörigen Zahlen die sämmtlichen Zahlen geben muss, welche zu dem Producte q gehören. Denn einmal erhellt aus dem Vorigen, dass jede solche Combination wirklich eine zu q gehörige Zahl giebt; es lässt sich ferner leicht nachweisen, dass sie alle nach dem Modul p von einander verschieden sind; endlich sind sie auch in der erforderlichen Anzahl vorhanden. Nämlich ihre Anzahl ist offenbar $S'''a^\alpha . S'''b^\beta . S'''c^\gamma$ .... und da man nach einem in der Einleitung bewiesenen Satze

$$S'''a^\alpha . S'''b^\beta . S'''c^\gamma \ldots . S'''q$$

hat, so ist dieselbe gleich der Anzahl von Zahlen, welche zu dem Exponenten q gehören.

Gehen wir zu dem Exponenten 8 über, so ist eine der zugehörigen Zahlen

$$A'^{\frac{p-1}{a^3}} = 5^9 \equiv -21 . 3 \equiv -63 \equiv 10,$$

also die vollständige Reihe derselben identisch mit den Potenzen

$$10^1,\ 10^3,\ 10^5,\ 10^7$$

oder, wenn wir die positiven kleinsten Reste nehmen,

$$10\quad 51\quad 63\quad 22.$$

Weiter für den Exponenten 9 erhalten wir zunächst die specielle Zahl

$$B'^{\frac{p-1}{b2}} = 2^8 \equiv 4 . -9 \equiv 37$$

und hieraus die Reihe sämmtlicher zugehörigen Zahlen

$$37\quad 37^2\quad 37^4\quad 37^5\quad 37^7\quad 37^8$$

oder, wenn man für 37 seinen Werth 2^8 setzt,

$$2^8\quad 2^{16}\quad 2^{32}\quad 2^{40}\quad 2^{56}\quad 2^{64};$$

die gesuchten Zahlen sind mithin

$$37\quad 55\quad 32\quad 16\quad 4\quad 2.$$

Für den Divisor 12 haben wir die Zahlen, die zu 3 und 4 respective gehören, mit einander zu combiniren, also die Zahlen -9 und $+8$ mit den Zahlen $+27$ und -27. Dies giebt 4 Combinationen, also die hinreichende Anzahl, da auch nicht mehr relative Primzahlen zu 12, die kleiner sind, existiren. Dieselben sind

$$-243,\ +243,\ +216,\ -216$$

und geben die positiven Reste

$$49\quad 24\quad 70\quad 3.$$

Für den Divisor 18 haben wir die zu 2 gehörige Zahl -1 mit den zu 9 gehörigen Zahlen

$$37\quad 55\quad 32\quad 16\quad 4\quad 2$$

zu combiniren; dies giebt

$$36\quad 18\quad 41\quad 57\quad 69\quad 71.$$

Wenn der Exponent 24 ist, so entspringen die 8 dazu gehörigen Zahlen durch Combination der zu 3 gehörigen Zahlen

$$-9\quad 8$$

mit den zu 8 gehörigen Zahlen

$$10\quad -22\quad -10\quad 22;$$

sie werden mithin

$$-90\quad +198\quad +90\quad -198\quad 80\quad -176\quad -80\quad +176$$

oder einfacher

$$56\quad 52\quad 17\quad 21\quad 7\quad 43\quad 66\quad 30.$$

Ist der Exponent 36, so hat man die zu 4 gehörigen Zahlen

$$+27\quad -27$$

mit den zu 9 gehörigen

$$-36 \quad -18 \quad +32 \quad +16 \quad 4 \quad 2$$

zu verbinden und erhält dadurch die 12 Zahlen:

$$\begin{array}{cccccc} -972 & -486 & +864 & 432 & 108 & 54 \\ +972 & +486 & -864 & -432 & -108 & -54 \end{array}$$

oder

$$\begin{array}{cccccc} 50 & 25 & 61 & 67 & 35 & 54 \\ 23 & 48 & 12 & 6 & 38 & 19. \end{array}$$

Endlich wenn der Exponent $72 = 8.9$ ist, so hat man

$$10 \quad 22 \quad -10 \quad -22$$

zu combiniren mit

$$-36 \quad -18 \quad 32 \quad 16 \quad 4 \quad 2.$$

Dies giebt die Zahlen

$$\begin{array}{cccccccccccc} -360 & -180 & 320 & 160 & 40 & 20 & -792 & -396 & 704 & 352 & 88 & 44 \\ +360 & +180 & -320 & -160 & -40 & -20 & +792 & +396 & -704 & -352 & -88 & -44 \end{array}$$

oder, wenn man die kleinsten positiven Reste nimmt:

$$\begin{array}{cccccccccccc} 5 & 39 & 28 & 14 & 40 & 20 & 11 & 42 & 47 & 60 & 15 & 44 \\ 68 & 34 & 45 & 59 & 33 & 53 & 62 & 31 & 26 & 13 & 58 & 29. \end{array}$$

Stellen wir jetzt die gewonnenen Resultate zusammen, so bekommen wir folgende Tabelle:

q	*mod* 73
1	1
2	72
3	8 64
4	27 46
6	9 65
8	10 22 51 63
9	2 4 16 32 37 55
12	3 24 49 70
18	18 36 41 57 69 71
24	7 17 21 30 43 52 56 66
36	6 12 19 23 25 35 38 48 50 54 61 67
72	5 11 13 14 15 20 26 28 29 31 33 34 39 40 42 44 45 47 53 58 59 60 62 68

Da die Anzahl der zu einem Exponenten gehörigen Zahlen gleich der Anzahl der relativen Primzahlen dazu, die kleiner als er sind, ist und

da die sämmtlichen Zahlen von 1 bis $p-1$ sich als zugehörige Zahlen auf die verschiedenen Divisoren von $p-1$ vertheilen, so erhellt sogleich, allerdings zunächst nur für solche Zahlen, die um 1 niedriger als eine Primzahl sind, der schon in der Einleitung bewiesene Satz: Wenn man sich die sämmtlichen Theiler einer gegebenen Zahl und zu jedem Theiler das zugehörige S''' aufsucht, so ist die Summe aller dieser S''' gleich der Zahl selbst.

Crelle hat in seiner „encyclopädischen Darstellung der Theorie der Zahlen“ eine solche Tabelle gegeben, welche alle Primzahlen von 3 bis 101 umfasst. Daraus entnehmen wir zur Uebung für den Anfänger noch folgende Rechnungsbeispiele für 61 und für die Primzahlen von 3 bis 37:

q	$p=61$
1	1
2	60
3	13 47
4	11 50
5	9 20 34 58
6	14 48
10	3 27 41 52
12	21 29 32 40
15	12 15 16 22 25 42 56 57
20	8 23 24 28 33 37 38 53
30	4 5 19 36 39 45 46 49
60	2 6 7 10 17 18 26 30 31 35 43 44 51 54 55 59

q	$mod=p=37$
1	1
2	36
3	10 26
4	6 31
6	11 27
9	7 9 12 16 33 34
12	8 14 23 19
18	3 4 21 25 28 30
36	2 5 13 15 17 18 19 20 22 24 32 35

q	$mod=p=29$
1	1
2	28
4	12 17
7	7 16 20 23 24 25
14	4 5 6 9 13 22
28	2 3 8 10 11 14 15 18 19 21 26 27

q	$mod=p=31$
1	1
2	30
3	5 25
5	2 4 8 16
6	6 26
10	15 23 27 29
15	7 9 10 14 18 19 20 28
30	3 11 12 13 17 21 22 24

q	$mod = p = 23$
1	1
2	22
11	2 3 4 6 8 9 12 13 16 18
22	5 7 10 11 14 15 17 19 20 21

q	$mod = p = 19$
1	1
2	18
3	7 11
6	8 12
9	4 5 6 9 16 17
18	2 3 10 13 14 15

q	$mod = p = 17$
1	1
2	16
4	4 13
8	2 8 9 15
16	3 5 6 7 10 11 12 14

q	$mod = p = 13$
1	1
2	12
3	3 9
4	5 8
6	4 10
12	2 6 7 11

q	$mod = p = 11$
1	1
2	10
5	3 4 5 9
10	2 6 7 8

p	$mod = p = 7$
1	1
2	6
3	2 4
6	3 5

p	$mod = p = 5$
1	1
2	4
4	2 3

3) Zur Vervollständigung unserer Theorie gehören noch folgende Theoreme:

I. Die Anzahl der zu irgend einem Exponenten gehörigen Zahlen ist immer eine gerade Zahl, ausgenommen den Fall, wo der Exponent gleich 1 oder 2 ist.

Dies folgt unmittelbar daraus, dass die Anzahl der Zahlen, welche kleiner als eine gegebene Zahl und relative Primzahlen dazu sind, eine gerade ist.

II. Wenn eine Zahl zu irgend einem Exponenten gehört, so existirt immer eine und zwar nur eine einzige Zahl, welche zu demselben Exponenten gehört, von der Beschaffenheit, dass das Product beider Zahlen die Einheit als Rest lässt. (Ausgenommen sind wieder die Exponenten 1 und 2).

So z. B. hat man, wenn man $p = 61$ und $q = 60$ hat, die Congruenzen:

$$\left.\begin{array}{r} 2.31 \equiv 1 \\ 6.51 \equiv 1 \\ 7.35 \equiv 1 \\ 10.55 \equiv 1 \\ 17.18 \equiv 1 \\ 26.54 \equiv 1 \\ 30.59 \equiv 1 \\ 43.44 \equiv 1 \end{array}\right\} (mod\ 61).$$

Um dieses zu beweisen gehe man davon aus, dass, wenn $m < q$ und relative Primzahl zu q ist, die Zahl $q-m$ gleichfalls relative Primzahl zu q sein muss (nach einem in der Einleitung bewiesenen Satze). Mithin, wenn die Zahl Q zu dem Exponenten q gehört, so sind irgend welche zwei andere dazu gehörige und von einander verschiedene Zahlen Q^m und Q^{q-m}; deren Product aber ist

$$Q^m . Q^{q-m} = Q^q \equiv 1 \ (mod\ p).$$

Wir müssen noch beweisen, dass es keine zweite zu q gehörige Zahl giebt, welche mit Q^m multiplicirt die Congruenz 1 befriedigt. Gäbe es eine solche Zahl $Q^{m'}$, wo der Exponent m' eine von $q-m$ verschiedene relative Primzahl $< q$ zu q sein könnte, so dass

$$Q^m . Q^{m'} = Q^{m+m'} \equiv 1$$

wäre, so müsste $m+m'$ ein Vielfaches von q sein. Das ist aber ein Widerspruch, da $m+m'$ der Annahme zu Folge zwischen den Grenzen 0 und $2q$ liegen muss, so dass es weder eine dieser Grenzen erreichen noch auch gleich q werden kann.

Hieraus folgt unmittelbar das Theorem:

III. Das Product aller zu einem Exponenten (der von 1 und 2 verschieden ist) gehörigen Zahlen ist mit der Einheit congruent.

Die einzige Zahl, welche zu dem Exponenten 2 gehört, ist $p-1 \equiv -1$. Ist nun q eine ungerade Zahl und $2q$ ein Theiler von $p-1$, so ergeben sich die zu $2q$ gehörigen Zahlen durch Multiplication von -1 in jede einzelne zu q gehörige Zahl; mithin müssen sie erhalten werden, indem man jede der letzteren von p abzieht, und es ergiebt sich daher der Satz:

IV. Wenn q eine ungerade Zahl und $2q$ ein Factor von $p-1$ ist, so lassen sich die zu diesen beiden Exponenten q und $2q$ gehörigen Zahlen dergestalt anordnen, dass sie einander paarweise zu dem p Modul ergänzen.

Wir haben am Ende des vorigen Paragraphen bewiesen, dass, wenn x zu q gehört, immer die Congruenz

$$1+x+x^2+x^3+ \ldots\ldots +x^{q-1} \equiv 0 \ (mod\ p)$$

statt habe; dieselbe reducirt sich für $q=4$ auf

$$1+x+x^2+x^3 \equiv 0 \ (mod\ p).$$

Nun ist aber, wenn x zu 4 gehört, nothwendig

$$x^4 \equiv 1 \ (mod\ p)$$

und hieraus folgt durch Ausziehung der Quadratwurzel, da das positive Vorzeichen unzulässig ist (vergleiche hierüber 4) *b*)):

$$x^2 \equiv -1 \ (mod\ p);$$

demgemäss reducirt sich die vorhergehende Congruenz 0 auf

$$x + x^3 \equiv 0 \ (mod\ p)$$

und wir können also, wenn x eine der beiden dem Exponenten 4 zugehörigen Zahlen ist, beide darstellen durch

$$+x \text{ und } -x.$$

Die einem Exponenten $4q$ entsprechenden Zahlen lassen sich nun, wenn q und 4 relative Primzahlen sind, bestimmen durch Multiplication dieser Zahlen $+x$ und $-x$ mit denjenigen, welche sich auf den Exponenten q beziehen. Dieselben müssen also, auf die kleinsten Reste reducirt, paarweise zusammen 0 geben und wir erhalten dadurch den Satz:

V. Wenn q eine relative Primzahl zu 4 und $4q$ ein Divisor von $p-1$ ist, so lassen sich die dem Exponenten $4q$ zugehörigen Zahlen in solche Gruppen zu je 2 theilen, die einander zu dem Modul ergänzen.

4) Es mögen jetzt noch die Perioden der Reste untersucht werden, welche entstehen, wenn man sich die aufeinanderfolgenden Potenzen einer beliebigen Zahl bildet.

Wenn eine Zahl x zu einem Exponenten q gehört und man bildet sich die Reihe ihrer aufeinanderfolgenden Potenzen

$$q \ q^2 \ q^3 \ q^4 \ q^5 \ q^6 \ \ldots\ldots,$$

so gehen die Reste nach einer $q$gliedrigen Periode fort, so dass jede q aufeinanderfolgende Potenzen verschiedene Reste lassen. Die Perioden bestehen für alle Zahlen, die zu denselben Exponenten gehören, aus den nämlichen Restzahlen und unterscheiden sich nur durch die Ordnung, in der diese Restzahlen aufeinander folgen.

Der erste Theil des Satzes ist geradezu in der Schlussnummer des vorigen Paragraphen bewiesen; der zweite lässt sich, wie folgt, erweisen. Wenn m eine relative Primzahl zu q und kleiner als q ist, so sind x und x^q zwei von einander verschiedene Zahlen, die zu dem Exponenten q ge-

hören und es sollen die sämmtlichen Zahlen, welche die Periode

$$x \; x^2 \; x^3 \; x^4 \; \ldots\ldots\ldots \; x^q$$

zusammensetzen, auch in der Periode

$$x^m \; x^{2m} \; x^{3m} \; \ldots\ldots\ldots \; x^{qm}$$

vorkommen. In der That greifen wir eine beliebige Potenz x^{nm} aus letzterer heraus, so muss dieselbe in der Fortsetzung der ersten Periode, deren Exponenten die aufeinander folgenden Zahlen sind, irgend einmal vorkommen, mithin muss sie auch geradezu in dieser selbst enthalten sein, weil die Fortsetzung ja keine neuen Reste, sondern nur eine Wiederholung der früheren Reste liefert.

Beispiele. Der Modul sei 73, so gehören 8 und 64 zu dem Exponenten 3 und die zugehörigen Restperioden sind:

8 —9 1
—9 8 1;

die Restperioden, welche den Zahlen 27 und 9 entsprechen, sind bezüglich

27 —1 —27 1,
9 8 —1 —9 —8 1;

Die Zahlen 2 und 37, 4 und 55, 16 und 32, welche alle zu dem ungeraden Exponenten 9 gehören, geben respective die Perioden:

2 4 8 16 32 —9 —18 —36 1 und
—36 —18 —9 32 16 8 4 2 1,
4 16 —9 —36 2 8 32 —18 1 und
—18 32 8 2 —36 —9 16 4 1,
16 —36 8 —18 4 —9 2 32 1 und
32 2 —9 4 —18 8 —36 16 1.

Endlich den Zahlen 10 und 22, 51 und 63, welche zu dem geraden Exponenten 8 gehören, entsprechen die Perioden

10 27 —22 —1 —10 —27 22 1 und
22 —27 —10 —1 —22 27 10 1,
—22 —27 10 —1 22 27 —10 1 und
—10 27 22 —1 10 —27 —22 1.

Da alle Perioden, die sich auf demselben Exponenten zugehörige Zahlen beziehen, dieselben Zahlen enthalten, so **müssen nothwendig, wenn man die eine berechnet hat, die übrigen sich daraus**

ableiten lassen und in der That kann dieses mit Leichtigkeit geleistet werden. Es sei z. B. die Periode für 2 gegeben und die für 55 soll entwickelt werden. Der Gang der Rechnung ist in folgenden Congruenzen ausgedrückt, die sich natürlich alle auf den Modul 73 beziehen:

$$55^1 \equiv -18,$$

$$\begin{array}{lllllll}
55^2 & \equiv (-18)^2 & \equiv (2^7)^2 & \equiv 2^9.2^5 & \equiv 2^5 & \equiv & 32, \\
55^3 & \equiv -18.32 & \equiv 2^7.2^5 & \equiv 2^9.2^3 & \equiv 2^3 & \equiv & 8, \\
55^4 & \equiv -18.8 & \equiv 2^7.2^3 & \equiv 2^9.2 & \equiv 2^1 & \equiv & 2, \\
55^5 & \equiv -18.2^1 & \equiv 2^7.2^1 & \equiv 2^8 & \equiv -36, & & \\
55^6 & \equiv -18.-36 & \equiv 2^7.2^8 & \equiv 2^9.2^6 & \equiv 2^6 & \equiv & -9, \\
55^7 & \equiv -18.-9 & \equiv 2^7.2^6 & \equiv 2^9.2^4 & \equiv 2^4 & \equiv & 16, \\
55^8 & \equiv -18.16 & \equiv 2^7.2^4 & \equiv 2^9.2^2 & \equiv 2^2 & \equiv & 4.
\end{array}$$

Aus der Betrachtung der vorliegenden Beispiele fliessen sogleich einige wichtige Folgerungen, von denen wir die nachfolgenden hervorheben:

a) Wenn eine Zahl x zu einem ungeraden Exponenten q gehört, so existirt in der Periode der darauf bezüglichen Potenzreste kein Rest gleich -1 und es ist mithin die Congruenz

$$x^\lambda \equiv -1 \ (mod\ p),$$

wo λ eine beliebige ganze Zahl bezeichnet, für keinen Werth von λ möglich.

Gäbe es einen solchen Rest -1, so dass

$$x^\lambda \equiv -1 \ (mod\ p),$$

so würde durch Quadrirung folgen:

$$x^{2\lambda} \equiv 1 \ (mod\ p).$$

Man bestimme sich jetzt den kleinsten positiven Rest von 2λ in Bezug auf den ungeraden Modul q: er sei λ', so ist

$$2\lambda = mq + \lambda'$$

und λ' auf jeden Fall eine Zahl zwischen den Grenzen 0 und q, so dass sie mit keiner dieser Grenzen selbst zusammenfallen kann; denn sonst ginge die gerade Zahl 2λ durch die ungerade Zahl q auf. Nun würde folgen:

$$x_2\lambda = x^{mq+\lambda'} \equiv x^{\lambda'} \equiv 1 \ (mod\ p);$$

mithin existirt eine Potenz kleiner als die kleinste x^q, welche den Rest 1 gäbe.

b) Wenn eine Zahl x zu einem geraden Exponenten q gehört, so ist in der Periode der auf x bezüglichen Potenzreste allemal einer, aber auch nur ein einziger Rest gleich -1 vorhanden und dieser Rest gehört zur Potenz $x^{\frac{q}{2}}$ oder allgemeiner zur Potenz

$$x^{nq+\frac{q}{2}}.$$

Die Potenz $x^{\frac{q}{2}}$ muss nothwendig irgend einen von 0 verschiedenen Rest lassen, um dessen Bestimmung es sich handelt, und dieser Rest muss ebenso nothwendig zu irgend einem von 0 verschiedenen Exponenten gehören, welcher ein Theiler von $p-1$ ist. Sei dieser Exponent q', so bestehen die beiden Congruenzen

$$\left.\begin{aligned} x^{\frac{q}{2}} &\equiv 1 \\ r^{q'} &\equiv 1 \end{aligned}\right\} (mod\ p).$$

Erhebt man die erste auf die q'te Potenz, so folgt durch Vergleichung mit der zweiten

$$x^{\frac{qq'}{2}} \equiv r^{q'} \equiv 1\ (mod\ p);$$

nun gehört aber x zu dem Exponenten q, also muss q ein Factor von $\frac{qq'}{2}$ sein; dies ist nicht anders möglich, als wenn q' entweder gleich 0 oder gleich 2 ist. Das erste ist, wie schon bemerkt, nicht möglich, also bleibt nur die Annahme $q'=2$ statthaft und r ist mithin gleich der Zahl, welche zu dem Exponenten 2 gehört. Diese Zahl ist aber selbstverständlich $p-1$; denn die erste Potenz von $p-1$ giebt -1 und die zweite Potenz ist mithin die erste, welche gleich 1 ist. Mithin ist der gesuchte Rest

$$r \equiv p-1 \equiv -1\ (mod\ p).$$

Dieser Satz pflegt gewöhnlich so bewiesen zu werden:

Wenn die Congruenz

$$x^q \equiv 1\ (mod\ p)$$

stattfindet, so muss das Product

$$x^q - 1 = (x^{\frac{q}{2}} - 1)(x^{\frac{q}{2}} + 1)$$

durch p ohne Rest theilbar sein; das ist nicht anders möglich, als wenn entweder

$$x^{\frac{q}{2}} - 1$$

oder

$$x^{\frac{q}{2}} + 1$$

durch p ohne Rest theilbar ist. Nun ist das erste nicht statthaft, weil x zu q gehört und also keine Potenz von x, deren Exponent unter q ist, die Einheit zum Reste lassen kann; mithin bleibt nur die letzte Annahme übrig, also

$$x^{\frac{q}{2}} \equiv -1 \ (mod\ p).$$

Gegen diesen Beweis kann nichts eingewandt werden, sobald ihm der allgemeine Beweis vorausgeht, dass wirklich zu jedem beliebigen Theiler q ein zugehöriges x existirt, d. h. dass die Congruenz

$$x^q \equiv 1 \ (mod\ p)$$

überhaupt möglich ist; er hat aber nicht die erforderliche Strenge, wenn er, wie es wohl zu geschehen pflegt, diesem Nachweise vorausgeht. Denn es wäre ja denkbar, dass die Congruenz sich in sich selber widerspräche und daher überhaupt nicht befriedigt werden könnte; dies vorausgesetzt würde aber gerade der umgekehrte Schluss, dass -1 kein Rest zu $x^{\frac{q}{2}}$ wäre, der allein statthafte sein.

c) Wenn man von der Periode der Reste, welche zu den Potenzen einer beliebigen (von 0 verschiedenen) Zahl gehört, das Endglied 1 wegwirft (also nur die $(q-1)$ten Glieder betrachtet), so sind die Producte je zweier Glieder, die gleich weit von den beiden Enden abstehen, immer solche Zahlen, die nach dem Modul p den Rest 1 geben.

Für den Beweis sind, streng genommen, zwei Fälle zu unterscheiden, nämlich der Fall eines ungeraden q und der Fall eines geraden q. Im ersteren Falle existirt für die betrachteten $(q-1)$ Glieder kein mittleres Glied, dagegen wohl im zweiten Fall. Indessen kann man dasselbe, weil es ja eben so weit von dem ersten Gliede, wie von dem $(q-1)$ten Gliede absteht, doppelt rechnen und dadurch beide Fälle wieder in einen zusammenbringen. Die Form zweier solcher Glieder, wie wir sie voraussetzen, ist dann

$$x^m, \ x^{q-m}$$

und man erhält sogleich, da x zu q gehört,

$$x^m . x^{q-m} = x^q \equiv 1 \ (mod\ p),$$

wie zu beweisen war.

Hieraus ergiebt sich unmittelbar weiter, dass das Product sämmtlicher eine Periode zusammensetzender Reste im Falle eines ungeraden q

gleich 1 und auch im Falle eines geraden q, wenn man das Mittelglied -1 doppelt rechnet. Dies ist näher das schon am Schlusse des vorigeu Paragraphen erwähnte Theorem:

Das Product sämmtlicher eine Periode bildenden Reste giebt, wenn q ungerade ist, $+1$ und, wenn q gerade ist, -1.

Beispiel. Für die Periode, welche sich auf die zu dem Exponenten 9 gehörige Zahl 37 bezieht, ist:

$$\left.\begin{array}{r} -36.\ 2 \equiv 1 \\ -18.\ 4 \equiv 1 \\ -\ 9.\ 8 \equiv 1 \\ -32.16 \equiv 1 \end{array}\right\} (mod\ 72).$$

d) Wenn 2 Zahlen x und x', deren Product den Rest 1 lässt, beide zu dem Exponenten q gehören, so ist die Periode der Reste, die sich auf die Potenzen der einen bezieht, das Umgekehrte von der Periode, die sich auf die Potenzen der andern bezieht. (Es wird hierbei natürlich von dem beiden Perioden gemeinschaftlichen Endgliede 1 wieder abgesehen.)

Der Satz spricht sich offenbar in der Congruenz

$$x^m \equiv x'^{q-m}\ (mod\ p)$$

aus. Um dieselbe zu erweisen, bemerken wir, dass, wenn man die aus der Voraussetzung fliessende Congruenz

$$xx' \equiv 1\ (mod\ p)$$

auf die $(q-m)$te Potenz erhebt, sich

$$x^{q-m} x'^{q-m} \equiv 1\ (mod\ p)$$

ergiebt; hieraus folgt, indem man auf beiden Seiten mit x^m multiplicirt,

$$x^q x'^{q-m} \equiv x^m$$

und diese Congruenz geht in die zu erweisende über, wenn man für x^q seinen Rest 1 setzt.

Die oben aufgeführten Perioden für die Reste der Zahlen, die den Exponenten 9 und 8 entsprechen, geben eine hinlängliche Menge von Beispielen für die Richtigkeit des Satzes.

e) Wenn man von irgend einer Periode eine beliebige Anzahl auf einander folgender Glieder herausgreift, so sind immer die Producte je zweier Glieder, die gleich weit von den beiden Enden abstehen, einander nach dem Modul p congruent.

Z. B. aus der der Zahl 4 entsprechenden Periode wollen wir alle Glieder vom zweiten ab für sich betrachten, also die Reihe

$$4 \quad 8 \quad 16 \quad 32 \quad -9 \quad -18 \quad -36 \quad 1;$$

und wir erhalten in der That die Congruenzen

$$\left.\begin{aligned} 4.\quad 1 &\equiv 4 \\ 8.-36 &\equiv 4 \\ 16.-18 &\equiv 4 \\ 32.-\ 9 &\equiv 4 \end{aligned}\right\} (mod\ 73),$$

welche leicht zu verificiren sind.

Betrachtet man ferner eine Reihe mit ungerader Gliederzahl, etwa

$$4 \quad 8 \quad 16 \quad 32 \quad -9,$$

so bestehen wiederum die Congruenzen

$$\left.\begin{aligned} 4.-9 &\equiv -36 \\ 8.\ 32 &\equiv -36 \\ 16.\ 16 &\equiv -36 \end{aligned}\right\} (mod\ 73).$$

Der allgemeine Beweis ist äusserst simpel. Sei die betrachtete Reihe

$$x^{\varkappa},\ x^{\varkappa+1},\ x^{\varkappa+2}, \ldots\ldots x^{\lambda-2},\ x^{\lambda-1},\ x^{\lambda},$$

so sind zwei beliebige gleich weit vom Ende abstehende Glieder

$$x^{\varkappa-\varepsilon},\ x^{\lambda-\varepsilon}$$

und man hat die identische Gleichung

$$x^{\varkappa}.x^{\lambda} = x^{\varkappa-\varepsilon}.x^{\lambda-\varepsilon},$$

aus welcher, wenn man für die einzelnen Potenzen ihre kleinsten Reste setzt, die zu beweisende Congruenz folgt.

f) Wenn man die sämmtlichen Glieder einer Restperiode auf die λte Potenz erhebt, so ist die Summe dieser Potenzen ein Vielfaches von dem Modul p, wenn q nicht in λ aufgeht, und dem Exponenten q congruent, wenn q in λ aufgeht.

Die genannte Summe ist

$$x^{\lambda}+x^{2\lambda}+x^{3\lambda}+\ldots.+x^{q\lambda} = 1+x^{\lambda}+x^{2\lambda}+x^{3\lambda}+\ldots.+x^{q\lambda-\lambda}$$

und mithin nach der bekannten Summenformel für eine geometrische Progression, deren Anfangsglied x^{λ} ist:

$$= \frac{x^{q\lambda}-1}{x^{\lambda}-1}$$

oder auch, da wegen der Congruenz

$$x^{q\lambda}-1 \equiv 0\ (mod\ p)$$

der Quotient

$$\frac{x^{q\lambda}-1}{p}$$

einer ganzen Zahl gleich sein muss, die wir mit G bezeichnen wollen,

$$x^{\lambda}+x^{2\lambda}+x^{3\lambda}+\ldots\ldots+x^{q\lambda}=\frac{Gp}{x^{\lambda}-1}.$$

Ist nun λ ein Vielfaches von q, so ist $x^{\lambda}-1$ ein Vielfaches von p, etwa

$$x^{\lambda}-1=gp$$

und der Quotient $\frac{Gp}{gp}$ wird alsdann auf keinen Fall ein Vielfaches von p werden können, indem sich p heraushebt, und es wird sein Werth dadurch gefunden werden, dass man untersucht, wie oft g in G enthalten ist. Einfacher kommt man aber unmittelbar durch Betrachtung der linken Seite zum Resultate, wo jede Potenz von x für den angezeigten Fall zum Reste 1 hat; mithin, da wir q solcher Potenzen haben, folgt

$$x^{\lambda}+x^{2\lambda}+\ldots.+x^{q\lambda}\equiv q \pmod p.$$

Ist dagegen λ kein Vielfaches von q, so ist $x^{\lambda}-1$ auch kein Vielfaches von p und mithin relative Primzahl zu p; die rechte Seite unserer Gleichung kann daher nur dadurch, wie sie es doch muss, eine ganze Zahl werden, dass $x^{\lambda}-1$ in G aufgeht, und wird also ein Vielfaches von d geben, so dass

$$x^{\lambda}+x^{\lambda}+x^{3\lambda}+\ldots.+x^{q\lambda}\equiv 0 \pmod p$$

wird.

Beispiel. Wenn wir die Primzahl 61 als Modul annehmen, so gehört zu dem Exponenten 6 die Zahl 14 und wenn wir uns die Periode der Reste bilden und darauf die respectiven Summen der 6 ersten Potenzen dieser Reste (wo natürlich diese Potenzen nur in ihren kleinsten Resten ausgedrückt werden), so erhalten wir wirklich:

$$\left.\begin{array}{r} 14+13-1-14-13+1\equiv 0\\ +13-14+1+13+14+1\equiv 0\\ -1+1-1+1-1+1\equiv 0\\ -14+13+1-14+13+1\equiv 0\\ -13-14-1+13-14+1\equiv 0\\ +1+1+1+1+1+1\equiv 6 \end{array}\right\} \pmod{61}.$$

§. 12.

Von den primitiven Wurzeln einer gegebenen Primzahl.

1) Aus den vorhergehenden Erörterungen ist klar, dass zu jedem Theiler von $p-1$ sich solche Zahlen finden lassen, welche zu ihm als Exponenten gehören. Unter den verschiedenen Fällen, welche den verschiedenen Theilern entsprechen, hebt sich nun einer ganz besonders hervor, nämlich der Fall, in welchem die zu $p-1$ selbst gehörigen Zahlen untersucht werden, und man hat darum für ihn eine besondere Bezeichnung eingeführt. Man nennt eine Zahl g, welche zu dem Exponenten $p-1$ gehört, eine primitive Wurzel der Primzahl p. Dieses vorausgesetzt können wir die sämmtlichen Sätze des vorigen Paragraphen sogleich auf die primitive Wurzel übertragen und erhalten dadurch namentlich folgende Theoreme:

Die primitive Wurzel einer Primzahl ist eine solche Zahl, dass sie zu einer niedrigeren als der $(p-1)$ten Potenz erhoben von der Einheit verschieden bleibt. Die Periode der Reste demgemäss, welche ihren auf einander folgenden Potenzen entsprechen, besteht aus $p-1$ Gliedern und muss daher, abgesehen von der Reihenfolge, die sämmtlichen Glieder der Zahlenreihe

$$1 \quad 2 \quad 3 \quad 4 \ldots\ldots p-1$$

enthalten.

Wenn wir irgend eine primitive Wurzel g für die Primzahl p gefunden haben, so finden wir alle übrigen primitiven Wurzeln, wenn wir uns alle solche Potenzen von g bilden, deren Exponenten kleiner als $p-1$ und relative Primzahlen zu $p-1$ sind.

Die Anzahl aller primitiven Wurzeln einer gegebenen Primzahl (3 ausgenommen) ist gerade und zwar, wenn die Zusammensetzung des $p-1$ aus seinen Primfactoren durch die Formel

$$p-1 = a^{\alpha} b^{\beta} c^{\gamma} \ldots\ldots$$

bestimmt ist, gleich

$$(p-1)\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots\ldots$$

Hiernach, wenn die Reihe der Zahlen, die kleiner als $p-1$ und relative Primzahlen dazu sind,

$$1 \quad m' \quad m'' \quad m''' \ldots\ldots p-2$$

ist, wird man sich die sämmtlichen primitiven Wurzeln zu p durch folgende Reihen darstellen können, in denen allen dieselben Potenzreste, nur in verschiedener Reihenfolge, wiederkehren:

$$\begin{array}{llllll}
g, & g^{m'}, & g^{m''}, & g^{m'''}, & \ldots\ldots & g^{p-2}, \\
g^{m'}, & g^{m'm'}, & g^{m'm''}, & g^{m'm'''}, & \ldots\ldots & g^{m'(p-2)}, \\
g^{m''}, & g^{m''m'}, & g^{m''m''}, & g^{m''m'''}, & \ldots\ldots & g^{m''(p-2)}, \\
g^{m'''}, & g^{m'''m'}, & g^{m'''m''}, & g^{m'''m'''}, & \ldots\ldots & g^{m'''(p-2)}, \\
\ldots & \ldots & \ldots & \ldots & & \\
\ldots & \ldots & \ldots & \ldots & & \\
g^{(p-2)}, & g^{(p-2)m'}, & g^{(p-2)m''}, & g^{(p-2)m'''}, & \ldots\ldots & g^{(p-2)(p-2)}.
\end{array}$$

Aehnlich, wie schon erwähnt, steht es mit den Reihen, welche die Potenzreste geben; es entsteht die Frage, wie man, wenn g^m und $g^{m'}$ zwei primitive Wurzeln von p bezeichnen, zu irgend einem Gliede $g^{\lambda m}$ der einen Reihe

$$g^m \quad g^{2m} \quad g^{3m} \quad g^{4m} \ldots\ldots g^{\lambda m} \quad g^{\lambda m+1} \ldots\ldots$$

das entsprechende Glied $g^{xm'}$ der andern Reihe

$$g^{m'} \quad g^{2m'} \quad g^{3m'} \quad g^{4m'} \ldots\ldots g^{xm'} \quad g^{xm'+1} \ldots\ldots$$

finden könne.

Zu dem Zwecke bestimme man sich zuerst die Entstehung der beiden Anfangsglieder auseinander, was immer ausgeführt werden kann, wenn man g^m und $g^{m'}$ nach und nach auf alle Potenzen erhebt, deren Exponenten relative Primzahlen zu $p-1$ und kleiner als $p-1$ sind. Auf diese Weise möge gefunden werden

$$\left.\begin{array}{l}(g^m)^a \equiv g^{am} \equiv g^{m'} \\ (g^{m'})^b \equiv g^{bm'} \equiv g^m\end{array}\right\} (mod\, p);$$

diese Congruenzen erhebe man respective auf die $x$te und λte Potenz, so folgt

$$\left.\begin{array}{l}g^{axm} \equiv g^{xm'} \\ g^{b\lambda m'} \equiv g^{\lambda m}\end{array}\right\} (mod\, p)$$

und hieraus ergiebt sich durch Vergleichung mit der Congruenz

$$g^{xm'} \equiv g^{\lambda m} \ (mod\, p),$$

welche die Gleichheit der beiden betrachteten Glieder ausdrückt.

$$\left.\begin{array}{l} g^{axm} \equiv g^{\lambda m} \\ g^{b\lambda m'} \equiv g^{xm'} \end{array}\right\} (mod\ p).$$

Diese Congruenzen werden zu Folge der Periodicität der Reste erfüllt, sobald

$$\left.\begin{array}{l} ax \equiv \lambda \\ b\lambda \equiv x \end{array}\right\} (mod = p - 1)$$

ist. Vermöge Auflösung der ersten Congruenz ist man im Stande den Uebergang von der ersten Reihe in die zweite und vermöge Auflösung der zweiten Congruenz den Uebergang von der zweiten Reihe in die erste zu bewerkstelligen.

Z. B. die primitiven Wurzeln von 11 sind zu Folge der Tabelle des vorhergehenden Paragraphen:

2 6 7 8

und die Perioden für die Potenzreste zweier davon, etwa der Zahlen 2 und 6, sind

$$\begin{array}{cccccccccc} +2 & +4 & -3 & +5 & -1 & -2 & -4 & +3 & -5 & +1 \\ -5 & +3 & -4 & -2 & -1 & +5 & -3 & +4 & +2 & +1 \end{array}$$

Man findet ohne Mühe durch Probiren

$$\left.\begin{array}{l} (+2)^9 \equiv -5 \\ (-5)^9 \equiv +2 \end{array}\right\} (mod\ 11),$$

also $a = 9$, $b = 9$ (dass a und b hier gleich werden, hängt damit zusammen, dass wir zwei solche primitive Wurzeln als Anfangsglieder gewählt haben, deren Product gleich Eins ist); mithin werden die Bedingungscongruenzen, welche den Zusammenhang beider Reihen ausdrücken

$$\left.\begin{array}{l} x \equiv 9\lambda \\ \lambda \equiv 9x \end{array}\right\} (mod\ 10).$$

Sei nun z. B. zu dem 3ten Gliede der ersten Reihe das entsprechende Glied der zweiten zu suchen, so ist die aufzulösende Congruenz, da $x = 3$,

$$3 \equiv 9\lambda\ (mod\ 10)$$

oder

$$1 \equiv 3\lambda\ (mod\ 10);$$

dieser Congruenz genügt

$$\lambda \equiv -3\ (mod\ 10)$$

und mithin ist das 7te, 17te, 27ste .... Glied der zweiten Reihe dem 3ten Gliede der ersten Reihe, nämlich —3, gleich, wie auch ein Blick auf dieselben bestätigt. Soll umgekehrt zu dem 4ten Gliede der zweiten Reihe

das entsprechende der ersten gefunden werden, so ist die aufzulösende Congruenz

$$4 \equiv 9x \ (mod\ 10);$$

derselben wird genügt durch

$$x \equiv -4 \ (mod\ 10),$$

also ist das $(10-4)=6$te Glied der ersten Reihe gleich dem 4ten Gliede der zweiten Reihe.

Die beiden Bedingungscongruenzen sind übrigens unter allen Umständen möglich, da a und b zu Folge der Natur ihrer Entstehung relative Primzahlen zu $p-1$ und kleiner als diese Zahl sind.

2) Das Product aller primitiven Wurzeln einer Primzahl ist gleich 1.

Dieser Satz ergiebt sich unmittelbar aus den Sätzen in der dritten Nummer des vorigen Paragraphen. Es geht aus derselben zugleich hervor, dass die sämmtlichen primitiven Wurzeln sich paarweise so gruppiren lassen, dass die Zahlen jedes Paares mit einander multiplicirt die Congruenz 1 befriedigen.

Ein anderer interessanter Satz, der aber nicht so unmittelbar aus dem Vorhergehenden entnommen werden kann, ist folgender:

Die Summe aller primitiven Wurzeln ist nach dem Modul p 0, wenn $p-1$ nicht aus lauter einfachen Primfactoren zusammengesetzt ist, und ist gleich ± 1, wenn $p-1$ nur aus einfachen Primfactoren sich zusammensetzt, nämlich gleich $+1$, wenn diese einfachen Primfactoren in gerader Anzahl, und gleich -1, wenn sie in ungerader Anzahl vorhanden sind.

Um ihn zu beweisen schicken wir den Satz voraus:

Die Summe aller zu dem Exponenten q gehörigen Zahlen giebt -1, wenn q eine Primzahl, und 0, wenn q eine von der ersten verschiedene Potenz einer Primzahl ist.

Sei nämlich x eine dem Exponenten q zugehörige Zahl, so ist nach dem Schlusssatze des vorigen Paragraphen in beiden Fällen:

$$1+x+x^2+x^3+\ldots+x^{q-1}\equiv 0 \ (mod.p).$$

Hieraus folgt für den ersten Fall unmittelbar

$$x+x^2+\ldots+x^{q-1}\equiv -1 \ (mod\ p),$$

d. h. die zu erweisende Congruenz, da alsdann alle Potenzen von x in dieser Reihe solche Zahlen geben, die zu q gehören.

Dagegen, wenn q von der Form a^α ist, wo a eine Primzahl bezeichnet, bemerke man, dass, weil x zu q gehört,

$$x^{a^\alpha} - 1 \equiv 0 \ (mod\ p)$$

und

$$x^a - 1$$

von 0 verschieden und daher relative Primzahl zu p sein muss. Mithin können wir die vorhergehende Congruenz durch den letzten Ausdruck dividiren und erhalten

$$\frac{x^{a^\alpha} - 1}{x^a - 1} \equiv 0 \ (mod\ p)$$

oder, wenn man die Division ausführt, nach einem bekannten Satze der Algebra:

$$1 + x^a + x^{2a} + x^{3a} + x^{a^\alpha - a} \equiv 0 \ (mod\ p).$$

Ziehen wir diese Congruenz von derjenigen, mit der wir den Beweis einleiteten, ab, so werden links nur diejenigen Glieder übrig bleiben, in denen die Exponenten von x keinen Factor mit $q = a^\alpha$ gemeinsam haben, d. h. es bleibt die Summe aller zu q gehörigen Zahlen als congruent mit 0 übrig. —

Nehmen wir jetzt $p - 1$ von der Form

$$p - 1 = a^\alpha \,.\, b^\beta \,.\, c^\gamma \ldots\ldots$$

an, so erhält man nach dem vorigen Paragraphen alle primitiven Wurzeln, wenn man die zu den Exponenten a^α, b^β, c^γ, ... gehörigen Zahlen in jeder nur möglichen Weise mit einander combinirt, so dass jede einzelne Combination je eine diesen Exponenten entsprechende Zahl enthält und das Product aller sie zusammensetzenden Zahlen ausdrückt. Diese Combinationen können aber alle als Glieder einer Summenreihe erhalten werden, welche man sich bildet, indem man die Summen aller respective auf a^α, b^β, c^γ, ... bezüglichen Zahlen mit einander multiplicirt; diese Summenreihe, d. h. die Summe aller auf $p - 1$ bezüglichen Zahlen, ist mithin gleich einem Producte, in welchem so oft der Factor -1 vorkommt, als $p - 1$ einfache Primfactoren besitzt, die nur in der ersten Potenz vorkommen, und so oft 0, als in $p - 1$ von der ersten verschiedene Potenzen einfacher Primfactoren vorkommen. Hierin liegt der zu erweisende Satz.

Uebrigens erhellt unmittelbar aus der Art des Beweises, dass er folgende Verallgemeinerung gestattet:

Die Summe aller zu dem Exponenten q gehörigen Zahlen ist 0, wenn q nicht aus lauter einfachen, nur in der ersten Potenz vorkommenden Primfactoren zusammengesetzt ist, und ist gleich ± 1, wenn q nur aus einfachen Primfactoren besteht, nämlich gleich $+1$, wenn die Anzahl dieser verschiedenen einfachen Primfactoren gerade, und -1, wenn diese Anzahl ungerade ist.

Beispiel:

q	$mod = p = 73$
2	$72 \equiv -1$
3	$8+64=72 \equiv -1$
$2^2=4$	$27+46=73 \equiv 0$
$2.3=6$	$9+65=74 \equiv +1$
$2^3=8$	$10+22+51+63=146 \equiv 0$
$3^2=9$	$2+4+16+32+37+55=146 \equiv 0$
$2^2.3=12$	$3+24+49+70=146 \equiv 0$
$2.3^2=18$	$18+36+41+57+69+71=292 \equiv 0$
$2^3.3=24$	$7+17+21+30+43+52+56+66=292 \equiv 0$

3) Wenn q irgend ein Theiler von $p-1$ und g irgend eine primitive Wurzel bezeichnet und man bildet sich der Reihe nach die Reste der Potenzen

$$g \quad g^2 \quad g^3 \quad g^4 \ldots\ldots\ldots g^{p-1},$$

so gehören alle diejenigen, deren Exponenten mit $p-1$ zum grössten gemeinschaftlichen Theiler die Zahl

$$q' = \frac{p-1}{q}$$

haben, zu dem Exponenten q. Man kann mithin, wenn eine primitive Wurzel gegeben ist, sich nicht blos die übrigen, sondern überhaupt alle Zahlen berechnen, die zu irgend welchen Exponenten gehören.

Die Reihe der Exponenten, welche die betrachteten Potenzen haben, ist

$$1 \quad 2 \quad 3 \quad 4 \ldots\ldots p-1.$$

Nehmen wir zunächst $q=p-1$, also $q'=1$ an, so sind alle Exponen-

ten, die zum grössten gemeinschaftlichen Theiler mit $p-1$ die Zahl 1 haben, keine anderen als die relativen Primzahlen zu $p-1$ und der Satz kommt mithin für diesen Fall auf das Frühere zurück.

In den übrigen Fällen, wenn q ein beliebiger Theiler von $p-1$ ist, wollen wir zunächst zeigen, dass er auf jeden Fall so viele Zahlen liefert, als möglicher Weise zu q gehören können. Nehmen wir irgend einen Exponenten e aus unserer Potenzreihe heraus, der mit $p-1$ zum grössten gemeinschaftlichen Theiler q' hat, so müssen die Quotienten

$$\frac{e}{q'} \text{ und } \frac{p-1}{q'} = q$$

nothwendig relative Primzahlen zu einander sein. Weiter ist e immer kleiner als

$$p-1 = qq',$$

also folgt die Ungleichung

$$\frac{e}{q'} < q.$$

Aus beiden zusammen ergiebt sich, dass $\frac{e}{q'}$ nicht mehr Werthe annehmen kann, als relative Primzahlen zu q existiren, die kleiner als diese Zahl sind. Nun kann man diesem Ausdrucke aber auch wirklich gerade so viele von einander verschiedene Werthe geben; denn man braucht zu diesem Zwecke nur e als das Multiplum von q' in die verschiedenen Zahlen m zu betrachten, welche kleiner als q und relative Primzahlen zu q sind. Also liefert der Satz in der That die hinreichende Menge von Zahlen und es ist nur die Frage, ob dieselben auch wirklich zu q gehören.

Dies fällt nicht schwer zu beweisen. Denn irgend ein e, welches er liefert, hat nach dem Vorigen die Form mq' und die zugehörige Potenz daher die Form $g^{mq'}$. Nun ist, wenn man

$$g^{mq'} \equiv r \ (mod\ p)$$

setzt, r immer von 1 verschieden, weil $mq' < p-1$ und g zu $p-1$ gehört. Wir erhalten hieraus durch Erhebung auf die $q$te Potenz

$$r^q \equiv g^{mqq'} = g^{m(p-1)} \equiv 1 \ (mod\ p),$$

und es ist daher nur noch zu beweisen, dass der Exponent q der niedrigste ist, für welchen eine Potenz von r der Einheit congruent wird. Wäre nicht q, sondern x der niedrigste Exponent, für welchen dies einträte, so müsste

$$r^x \equiv g^{mq'x} \equiv 1 \pmod{p}$$

sein, mithin, da g eine primitive Wurzel ist, $mq'x$ ein Vielfaches von $p-1=qq'$. Dies ist nur möglich, wenn mx ein Vielfaches von q wäre, und da m und q relative Primzahlen zu einander sind, so würde hieraus folgen, dass x ein Vielfaches von q sein müsste, im offenbaren Widerspruche zu dem Satze, dass, wenn x zu r gehört, umgekehrt q ein Vielfaches von x sein muss.

Vermittelst dieses Theoremes ist es leicht sich eine praktische Regel abzuleiten für die Ausscheidung aller Zahlen aus der Reihe der Potenzen von g, welche zu dem Exponenten q gehören: Man suche alle nur möglichen Zahlen, welche kleiner als q und relative Primzahlen dazu sind, und multiplicire dieselben mit

$$q' = \frac{p-1}{q};$$

die hierdurch hervorgehenden Zahlen sind die Exponenten aller solcher Potenzen von g, deren Reste zu dem Divisor q gehören.

Beispiel. Der zu untersuchende Modul sei die Primzahl 61. Eine primitive Wurzel davon ist 2. Man bilde sich nun zunächst alle auf einander folgenden Potenzen von

$$g = 2$$

bis zur 60ten inclusive und erhält dadurch nachfolgende Tabelle, in der links die Exponenten von 2 und rechts die zugehörigen Reste stehen, und in der solche Reste, die primitive Wurzeln sind, mit einem Stern bezeichnet sind:

Exponenten von $g = 2$	Reste nach $mod = 61$	Exponenten von $g = 2$	Reste nach $mod = 61$
1	2	10	—13
2	4	11	—26*
3	8	12	9
4	16	13	18*
5	—29	14	—25
6	3	15	11
7	6*	16	22
8	12	17	—17*
9	24	18	27

Exponenten von $g = 2$	Reste nach $mod = 61$	Exponenten von $g = 2$	Reste nach $mod = 61$
19	— 7*	40	13
20	—14	41	26*
21	—28	42	— 9
22	5	43	—18*
23	10*	44	25
24	20	45	—11
25	—21	46	—22
26	19	47	17*
27	—23	48	—27
28	15	49	7*
29	30*	50	14
30	— 1	51	28
31	— 2*	52	— 5
32	— 4	53	—10*
33	— 8	54	—20
34	—16	55	21
35	29	56	—19
36	— 3	57	23
37	— 6*	58	—15
38	—12	59	—30*
39	—24	60	1

Die den einzelnen Divisoren q von $p-1$ entsprechenden Potenzexponenten, für welche die rechts nebenstehenden Zahlen zu q gehören, sind alsdann in folgender Tabelle enthalten:

q'	q	$e = mq'$															
1	60	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
2	30	1. 2	7. 2	11. 2	13. 2	17.2	19.2	23.2	29.2								
3	20	1. 3	3. 3	7. 3	9. 3	11.3	13.3	17.3	19.3								
4	15	1. 4	2. 4	4. 4	7. 4	8.4	11.4	13.4	14.4								
5	12	1. 5	5. 5	7. 5	11. 5												
6	10	1. 6	3. 6	7. 6	9. 6												
10	6	1.10	5.10														
12	5	1.12	2.12	3.12	4.12												
15	4	1.15	3.15														
20	3	1.20	2.20														
30	2	1.30															
60	1	0.60															

Sucht man jetzt die den bezeichneten Exponenten entsprechenden Reste, so erhält man dieselben Resultate, die in der Tabelle des vorigen Paragraphen sich verzeichnet finden, vermittelst der kleinsten Reste ausgedrückt.

Das eben erörterte Verfahren, die Zahlen von 1 bis $p-1$ auf die ihnen zugehörigen Exponenten zu vertheilen, gewährt vor demjenigen, welches wir im vorigen Paragraphen auseinandergesetzt haben, mannigfaltige Vortheile. Zwar hat man bei dem letzteren nicht so viel zu experimentiren, um für die Rechnung eine sichere Grundlage zu gewinnen; dagegen liefert das erstere zu gleicher Zeit die vollständige Restperiode für alle Potenzen einer primitiven Wurzel, aus denen man einmal mit leichter Mühe die den übrigen primitiven Wurzeln entsprechenden Restperioden berechnen kann, dann aber auch diejenigen, welche irgend einer andern Zahl entsprechen. Zu dem Zwecke hat man nur nöthig die Zahl a, deren Potenzreste man gerade haben will, in der Reihe der Reste aufzusuchen: sei die links daneben stehende Zahl α, so ist

$$a = g^{\alpha}$$

und vermittelst dieser Gleichung kann man alle Potenzen von a sich in Potenzen von g verwandeln, deren Reste man sogleich aus der Tabelle entnimmt.

Sei z. B. die Periode für

$$a = 41$$

zu bestimmen, so findet man

$$\begin{aligned}
41 &\equiv -20 \equiv 2^{54} \equiv -20 \\
41^{2} &\equiv 2^{108} \equiv 2^{48} \equiv -27 \\
41^{3} &\equiv 2^{54+48} \equiv 2^{42} \equiv -9 \quad (mod\ 61) \\
41^{4} &\equiv 2^{54+42} \equiv 2^{36} \equiv -3 \\
41^{5} &\equiv 2^{54+36} \equiv 2^{30} \equiv -1
\end{aligned}$$

Wenn man auf -1 gekommen ist, so müssen sich alle Reste mit entgegengesetztem Vorzeichen wiederholen und man hat daher ohne alle Rechnung die letzte Hälfte der Restperiode wie folgt:

$$\begin{aligned}
41^{6} &\equiv 20 \\
41^{7} &\equiv 27 \\
41^{8} &\equiv 9 \quad (mod\ 61). \\
41^{9} &\equiv 3 \\
41^{10} &\equiv 1
\end{aligned}$$

Hiernach ist klar, welchen ausserordentlichen Nutzen eine Tabelle solcher auf eine Basis g bezüglicher Restperioden für alle Primzahlen von 3 etwa bis 1000 gewähren würde. Die Einrichtung könnte dem Schema für 61 analog sein; nur müsste zu jeder Primzahl noch eine Tabelle hinzukommen, in welcher die Reste nach ihrer Grösse geordnet etwa rechts und links daneben die zugehörigen Exponenten stünden. Dies gäbe für $p = 61$ folgendes Schema:

Exponenten von $g=2$		Reste der zugehörigen Potenzen (*mod* 61)		Exponenten von $g=2$		Reste der zugehörigen Potenzen (*mod* 61)		Exponenten von $g=2$		Reste der zugehörigen Potenzen (*mod* 61)	
60	30	1	—1	15	45	11	—11	55	25	21	—21
1	31	2	—2	8	38	12	—12	16	46	22	—22
6	36	3	—3	40	10	13	—13	57	27	23	—23
2	32	4	—4	50	20	14	—14	9	39	24	—24
22	52	5	—5	28	58	15	—15	44	14	25	—25
7	37	6	—6	4	34	16	—16	41	11	26	—26
49	19	7	—7	47	17	17	—17	18	48	27	—27
3	33	8	—8	13	43	18	—18	51	21	28	—28
12	42	9	—9	26	56	19	—19	35	5	29	—29
23	53	10	—10	24	54	20	—20	29	59	30	—30

Diese Tabellen sind wirklich berechnet worden für alle Primzahlen, sowie für alle Potenzen von Primzahlen als Moduls, deren Werth die Zahl 1000 nicht übersteigt. Sie sind niedergelegt in dem „Canon arithmeticus" Berlin 1839, herausgegeben von dem berühmten Jacobi. Um eine feste Bezeichnung zu haben, ist daselbst nach Gauss' Vorgange der Exponent derjenigen Potenz von g, welche nach einem Modul p die gegebene Zahl a zum Reste hat, der Index dieser Zahl genannt. Hiernach sind z. B. die Gleichungen

$$3 = ind.\, 8, \quad 40 = ind.\, 13$$

identisch mit den Congruenzen

$$2^8 \equiv 3, 2^{40} \equiv 13 \pmod{61}$$

oder auch, wenn, wie in dem angeführten Werke, die Basis der auf den Modul 61 bezüglichen Indices nicht die primitive Wurzel 2, sondern die primitive Wurzel 10 ist,

$$16 = ind\, 8, \quad 31 = ind\, 13$$

identisch mit

$$10^{16} \equiv 8, \quad 10^{21} \equiv 13 \ (mod\, 61).$$

Um eine Idee von dem Vortheil solcher Tabellen zu geben, wollen wir an einem Beispiele ihre Anwendung zur Auflösung der Congruenzen ersten Grades erörtern. Sei die aufzulösende Congruenz von der Form

$$ax \equiv b \ (mod\, 61),$$

so bestimmen sich vermöge der zweiten Tabelle die Grössen α und β derartig, dass

$$a = 2^{\alpha}, \ b = 2^{\beta}$$

wird; so hat man

$$2^{\alpha} x \equiv 2^{\beta} \ (mod\, 61)$$

und hieraus unmittelbar

$$x \equiv 2^{\beta - \alpha} \ (mod\, 61);$$

indem man den Exponenten $\beta - \alpha$ in der ersten Tabelle links sucht, findet man den zugehörigen Werth von x, in dem kleinsten Reste ausgedrückt, rechts daneben. Sollte $\beta - \alpha$ sich negativ ergeben, so kann man ein solches Vielfache von

$$p - 1 = 60$$

hinzufügen, dass es positiv und kleiner als 60 wird; denn da 2 eine primitive Wurzel von 61 ist, so ist die zugehörige Restperiode 60gliedrig, mithin, wenn n eine beliebige ganze positive Zahl bezeichnet:

$$2^{\beta - \alpha} \equiv 2^{60n + \beta - \alpha}.$$

Um ein Beispiel in bestimmten Zahlen zu haben, legen wir die Congruenz

$$43x \equiv 23 \ (mod\, 61)$$

zur Auflösung vor; die zweite Tabelle giebt

$$43 \equiv -18 \equiv 2^{43},$$
$$23 \equiv 2^{57}$$

also

$$x \equiv 2^{57-43} \equiv 2^{14} \ (mod\, 61);$$

aus der ersten Tabelle erfahren wir jetzt, dass

$$x \equiv -25 \ (mod\, 61)$$

die Auflösung der gesuchten Congruenz ist und dies Resultat lässt sich leicht verificiren.

Sei ferner

$$128x \equiv 273 \ (mod\, 61),$$

so ist der Gang der Auflösung folgender:

$$\left.\begin{array}{l}128 \equiv -6 \equiv 2^{27} \\ 273 \equiv 29 \equiv 2^{35}\end{array}\right\} (mod\ 61)$$

mithin

$$x \equiv 2^{-2} \equiv 2^{60-2} \equiv 2^{58} \equiv -15\ (mod\ 61).$$

Wir begnügen uns mit diesen Andeutungen und übergehen das mannigfaltige Detail der übrigen Anwendungen, welche diese Tabellen zuliessen. Nur die eine Bemerkung, welche schon Gauss gemacht hat, fügen wir noch hinzu, dass diese Tafeln in der Zahlentheorie ungefähr dieselbe Rolle spielen dürften, wie die Logarithmen in der gemeinen Arithmetik und Algebra. Der Hauptvortheil, den die Logarithmen gewähren, besteht darin, dass man die Zahlen als Potenzen einer und derselben Basis erhält; gerade dasselbe wird auch vermöge der primitiven Wurzeln geleistet. Aber während dort unendlich viele Basen existiren, von denen allerdings nur eine in Anwendung zu kommen pflegt, sind hier nur eine beschränkte Anzahl von Basen vorhanden, aus denen man indessen ebenso wie dort nur eine, gleichgiltig welche, sich zum Gebrauche auswählt. Doch tritt wieder eine unendliche Mannigfaltigkeit dadurch in diese Art des Calculs hinein, dass die Base in engster Abhängigkeit mit dem Modul varirt, und gerade die wechselnde Natur der Aufgabe die Wahl des Moduls bestimmt, auf welchen man die Basis bezieht.

4) Wir wollen jetzt mit Hülfe der aufgestellten Principien den Satz von Wilson beweisen. Derselbe lautet wie folgt:

Wenn p eine Primzahl ist, so ist das Product

$$1.2.3.4\ \ldots.. (p-1 \equiv -1\ (mod\, p).$$

Sei g eine primitive Wurzel von p, so werden die Potenzen

$$g\quad g^2\quad g^3 \ldots.\ g^{p-1}$$

nach dem Modul p alle verschiedenen Reste lassen und dieselben mit den Zahlen der Reihe

$$1\quad 2\quad 3\ \ldots\ldots\ p-1$$

übereinstimmen. Nun giebt aber nach einem Lehrsatze in der letzten Nummer des vorigen Paragraphen unter $c)$ das Product sämmtlicher eine Periode bildenden Potenzreste $+$ oder -1, je nachdem die Gliederzahl ungerade oder gerade ist. Da nun $p-1$ immer eine gerade Zahl, so ist in unserm Falle das erwähnte Product -1, also unmittelbar die vorgelegte Congruenz erwiesen.

Ein anderer, analytischer Beweis desselben Satzes ist folgender: Betrachten wir die Reihe der Potenzen

$$1 \quad 2^{p-1} \quad 3^{p-1} \ldots\ldots (p-1)^{p-1} \quad p^{p-1} \ldots\ldots,$$

so ist bekannt, dass dieselbe eine arithmetische Reihe der $(p-1)$ten Ordnung bildet, d. h. wenn man sich die auf einander folgenden Differenzreihen bildet, so werden die Glieder der $(p-1)$ten alle unter einander und, wie man weiss, dem Producte

$$1.2.3 \ldots\ldots (p-1)$$

gleich sein. Andererseits aber kann man durch Induction leicht die allgemeine Form auffinden, unter der die Anfangsglieder einer jeden Differenzreihe stehen und indem man diese Form unserm Producte gleich setzt, erhält man

$$1.2.3. \ldots\ldots (p-1) = p^{p-1} - \frac{p-1}{1}(p-1)^{p-1} + \frac{p-1}{1}\frac{p-2}{2}(p-2)^{p-1}$$
$$-\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}(p-3)^{p-1} + \ldots\ldots - \frac{p-1}{1}2^{p-1} + 1.$$

Nun hat man nach dem Theoreme von Fermat

$$2^{p-1},\ 3^{p-1},\ \ldots\ldots (p-1)^{p-1} \equiv 1,\ p^{p-1} \equiv 0\ (mod\ p),$$

mithin ergiebt sich aus der vorhergehenden Gleichung die Congruenz

$$1.2.3.4 \ldots\ldots p-1 \equiv -\frac{p-1}{1} + \frac{p-1}{1}.\frac{p-2}{2} - \frac{p-1}{1}.\frac{p-2}{2}\frac{p-3}{3} + \ldots\ldots$$
$$-\frac{p-1}{1} + 1$$
$$\equiv -1 + \left(1 - \frac{p-1}{1} + \frac{p-1}{1}.\frac{p-2}{2} - \ldots\ldots - \frac{p-1}{1} + 1\right).$$

Aber nach einem bekannten Satze ist die auf der rechten Seite eingeklammerte Reihe gleich 0 und es folgt daher die Congruenz, welche den Satz von Wilson ausdrückt.

Es möge noch ein dritter Beweis hier Platz finden.

Wenn wir die Congruenz

$$x^{p-1} - 1 \equiv 0\ (mod\, p)$$

betrachten, so kann, da p eine Primzahl ist, dieselbe nicht mehr als höchstens $p-1$ unter einander verschiedene Wurzeln haben; nun genügen ihr aber nach dem Satze von Fermat die Zahlen

$$x = 1,\ 2,\ 3,\ 4,\ \ldots\ldots (p-2)(p-1),$$

deren Anzahl $p-1$ und die alle von einander verschieden sind; mithin

müssen dies die sämmtlichen Wurzeln unserer Gleichung sein. Hiernach muss man

$$x^{p-1}-1 \equiv (x-1)(x-2)(x-3) \ldots . (x-\overline{p-1})$$

haben, indem beide Formen äquivalent sind (cf. §. 9). Denken wir uns nun das Product rechts entwickelt und vergleichen die Coefficienten der gleich hohen Potenzen von x, so ergiebt sich, dass die Summe der Combinationen zu 1, 2, 3, 4, ... $(p-2)$ Elementen aus den Zahlen von 1 bis $p-1$ der Congruenz 0 genügt und dass man endlich für das letzte Glied

$$-1 \equiv -1.-2.-3.-4. \ldots . -(p-1)$$

hat, woraus, da die Anzahl der Minuszeichen rechts eine gerade ist, der Satz unmittelbar fliesst.

Beispiele.

$$1.2.3.4 = 24 \equiv -1 \ (mod\, 5).$$

$$1.2.3.4.5.6 = 720 \equiv -1 \ (mod\, 7).$$

$$1.2.3.4.5.6.7.8.9.10 = 3628800 \equiv -1 \ (mod\, 11).$$

Zum Schlusse dieses Paragraphen noch eine Notiz über eine nicht uninteressante Einzelheit. In der Einleitung haben wir erwähnt, dass Euler im Widerspruche zu einem von Fermat aufgeführten, aber nicht bewiesenen Satze dargethan hat, dass die Zahl

$$2^{32}+1$$

keine Primzahl sei. Sein Beweis dafür nimmt folgenden Gang. Ist die genannte Zahl keine Primzahl, so muss sie das Vielfache irgend einer Primzahl p sein, also

$$2^{32} \equiv -1 \ (mod\, p).$$

Hieraus ergiebt sich durch Quadrirung

$$2^{64} \equiv 1 \ (mod\, p);$$

mithin muss 64 nothwendig ein aliquoter Theil von $p-1$ sein, also p von der Form

$$p = 64n + 1.$$

Hat also unsere zu untersuchende Zahl einen Factor, so muss derselbe die eben gefundene Form haben. Indem Euler nun die Zahlen dieser Form durchprobirte, fand er, dass

$$2^{32}+1 = 4294967297 = 641 . 6700417$$

ist.

§. 13.

Theorie der allgemeinen Congruenz $x^n \equiv a \pmod{p}$.

1) Wenn wir q als einen Factor von $p-1$ annehmen, so können nicht mehr als höchstens q von einander verschiedene Werthe der Congruenz

$$x^q \equiv 1 \pmod{p}$$

genügen. Wenn wir nun für x der Reihe nach alle möglichen Zahlen von 1 bis $p-1$ einsetzen, folgt, dass nur ein Theil der dadurch entstehenden Potenzen den Rest 1 und die übrigen von 1 verschiedene Reste lassen müssen. Ueber die Natur dieser Reste giebt nun folgendes Theorem Aufschluss:

Wenn q ein Factor von $p-1$ ist und man setzt für x der Reihe nach die Zahlen

$$1 \; 2 \; 3 \; 4 \ldots\ldots p-1$$

ein, so erhält man (immer nach dem Modul p) $\frac{p-1}{q}$ verschiedene Reste der Potenz x^q, die zu je q von einander verschiedenen Werthen des x gehören.

Ehe wir den Satz beweisen, möge ein Beispiel ihn veranschaulichen, in welchem wir die Reste der Potenz x^3 nach dem Modul 31 betrachten.

Werthe der Potenz $x^3 \equiv r \pmod{31}$.

Rest r	Werthe der x	Rest r	Werthe der x	Rest r	Werthe der x
1	1 5 25	11		—10	
2	4 7 20	12		— 9	
3		13		— 8	12 21 29
4	16 18 28	14		— 7	
5		15	17 22 23	— 6	
6		—15	8 9 14	— 5	
7		—14		— 4	3 13 15
8		—13		— 3	
9		—12		— 2	11 24 27
10		—11		— 1	6 26 30

Die verschiedenen Reste, welche x^3 zulässt, vertheilen sich in $\frac{30}{3} = 10$

Gruppen zu je 3 von einander nach dem Modul 31 verschiedenen Werthen des x. Da wir, indem wir weiter gehen, keine von den vorigen verschiedene Reste bekommen können, so ergiebt sich unmittelbar, dass man für x keine Werthe angeben kann, für welche $x^3 \equiv 3, 5, 6, 7, \ldots.$ werden könnte.

Zunächst bestimme man sich irgend eine der zu q gehörigen Zahlen k, was nach dem Vorhergehenden immer möglich ist: dann sind die Potenzen

$$1 \;\; k \;\; k^2 \ldots\ldots k^{q-1}$$

alle von einander verschieden und genügen der Congruenz

$$x^q \equiv 1 \pmod p;$$

denn sei irgend eine derselben k^a, so ist

$$(k^a)^q = (k^q)^a \equiv 1 \pmod p;$$

mithin, da wir dadurch q von einander verschiedene Auflösungen bekommen und die Congruenz überhaupt nicht mehr zulässt, sind überhaupt keine davon verschiedene Zahlen vorhanden, welche den Rest 1 lassen könnten. Nehmen wir also irgend eine von den eben bestimmten verschiedene Zahl m, so wird dieselbe einen von 1 verschiedenen Rest r lassen, so dass

$$m^q \equiv r \pmod p.$$

Jetzt bilde man sich die Reihe

$$m \;\; mk \;\; mk^2 \;\; mk^3 \ldots\ldots mk^{q-1},$$

so sind diese q Zahlen alle von einander nach dem Modul p verschieden; denn wären zwei einander congruent, etwa

$$mk^e \equiv mk^\varepsilon \pmod p,$$

so folgte durch Division mit m, die zulässig, weil m und p relative Primzahlen sind,

$$k^e \equiv k^\varepsilon \pmod p,$$

d. h. k^e und k^ε wären einander gleich, im Widerspruche damit, dass alle Potenzen von k bis zur $(q-1)$ten hin einander incongruent sind. Ferner genügen sie alle der Congruenz

$$x^q \equiv r \pmod p;$$

denn setzt man irgend eine, etwa mk^e für x, so folgt

$$(mk^e)^q = m^q(k^q)^e \equiv r \pmod p.$$

Also, da nicht mehr als q Lösungen möglich sind, stellen sie die sämmt-

lichen von einander verschiedenen Zahlen dar, welche den Rest r geben können, und alle Zahlen, welche weder in der Reihe der Zahlen, die den Rest 1 geben, noch in dieser letzten Zahlenreihe mit inbegriffen sind, müssen nothwendig einen von 1 und r verschiedenen Rest r' haben.

Sei eine derselben m', so findet man wieder q verschiedene Zahlen, unter denen m' mit inbegriffen, welche dem Reste r' entsprechen, nämlich

$$m' \quad m'k \quad m'k^2 \; \ldots . \; m'k^{q-1}.$$

Indem man so weiter fortgeht, erhält man so lange immer neue Gruppen zu q Zahlen, die von den früheren verschiedene Reste lassen, als überhaupt noch Zahlen für die Untersuchung übrig bleiben. Offenbar aber, da q in $p-1$ aufgeht, indem

$$p-1 = qq'$$

werden keine von den $(p-1)$ Zahlen

$$1 \quad 2 \quad 3 \quad 4 \; \ldots . . \; p-1$$

mehr übrig sein können, wenn man den q'ten von den früheren verschiedenen Rest betrachtet hat. Also existiren überhaupt nur q' verschiedene Reste, die möglicher Weise bleiben können und jedem Reste entsprechen q von einander verschiedene Zahlen, durch welche er erzeugt werden kann.

In unserem Zahlenbeispiele bestimme man sich zuerst die dem Reste 1 entsprechenden Lösungen. Da 5 zu dem Exponenten 3 gehört, so sind das die Zahlen der Reihe

$$1 \quad 5 \quad 25.$$

Hierauf setze man für x einen beliebigen Zahlenwerth, der nicht mit einem der genannten zusammenfällt, etwa 2 ein und erhält dadurch

$$2^3 \equiv 8 \; (mod \; 31);$$

mithin geben die Zahlen

$$2 \quad 10 \quad 50$$

oder

$$2 \quad 10 \quad 19$$

den Rest 8. Aehnlich findet man für $x=3$, 4 die Reste -4 und $+2$ und denen entsprechend die Zahlen

$$3 \quad 15 \quad 75,$$

$$4 \quad 20 \quad 100$$

oder einfacher

$$3 \quad 15 \quad 13$$

$$4 \quad 20 \quad 7.$$

Die Zahl 5 ist nun bereits da gewesen; also untersucht man den Rest von 6^3. Er ist -1 und die bezüglichen Zahlen sind

$$6 \quad 30 \quad 150$$

oder

$$6 \quad 30 \quad 26.$$

Weiter erhält man für 8, da 7 schon vorgekommen, den Rest $-15 \equiv 2^3$ und die Zahlen

$$8 \quad 40 \quad 200$$

oder

$$8 \quad 9 \quad 14$$

und indem man so weiter fortgeht für die Reste

$$-2 \quad -8 \quad 4 \quad 15,$$

welche den Potenzen

$$11^3 \quad 12^3 \quad 16^3 \quad 17^3$$

entsprechen, bezüglich die Zahlenreihen:

$$11 \quad 24 \quad 27$$
$$12 \quad 21 \quad 29$$
$$16 \quad 18 \quad 28$$
$$17 \quad 22 \quad 23.$$

Indem, wie wir gesehen haben, die Potenz x^q nur

$$q' = \frac{p-1}{q}$$

verschiedene Zahlenwerthe bekommen kann, erhellt unmittelbar, dass von den Zahlen

$$1 \quad 2 \quad 3 \ldots . \; p-1$$

nothwendig eine Anzahl solcher Zahlen übrig bleiben muss, welche für keinen speciellen Werth des x der Potenz x^q congruent werden, so dass, wenn b eine solche Zahl ist, die Congruenz

$$x^q \equiv b \; (mod \; p)$$

überhaupt durch keine ganzzahligen Werthe von x befriedigt werden kann. Hiermit drängt sich die Frage auf: Wenn für eine gewisse Primzahl p als Modul irgend eine Zahl $b < p$ uns vorgelegt ist, unter welchen Bedingungen ist es möglich solche Zahlenwerthe für x zu bestimmen, welche die Potenz x^q der Zahl b congruent machen? oder mit andern Worten: wie entscheidet man, ob, unter der Voraussetzung, dass q ein Factor von $p-1$ ist, eine gegebene Zahl Rest oder Nichtrest zu einer gegebenen Potenz x^q ist?

Sei also wieder

$$qq' = p - 1,$$

so folgt, wenn die Congruenz

$$x^q \equiv b \ (mod\ p)$$

bestehen kann, durch Erhebung auf die q'te Potenz

$$x^{qq'} \equiv b^{q'} \ (mod\ p),$$

mithin, da nach Fermat's Fundamentaltheorem

$$x^{qq'} = x^{p-1} \equiv 1 \ (mod\ p)$$

ist:

$$b^{q'} \equiv 1 \ (mod\ p);$$

die letztgenannte Congruenz ist mithin eine nothwendige Folge des Bestehens der ersten. Aber man kann auch umgekehrt behaupten, dass, wenn dieser Congruenz Genüge geschehen kann, immer ein solcher Zahlenwerth für x sich bestimmen lässt, durch den die erste Congruenz gleichfalls befriedigt wird.

In der That, die Potenz x^q giebt, wie wir gesehen haben, q' verschiedene Reste, die unter allen Umständen genau bestimmt werden können, nämlich:

$$a'\ a''\ a''' \ldots\ldots a^{(q')};$$

also die Congruenz

$$x^q \equiv a \ (mod\ p)$$

ist nur dann nach x auflösbar, wenn a einem dieser q' verschiedenen Werthe congruent ist. Diese q' Werthe sind aber auch sämmtlich Lösungen der Congruenz

$$a^{q'} \equiv 1 \ (mod\ p),$$

weil die letztere eine Folge der vorhergehenden ist. Wäre demgemäss zu gleicher Zeit

$$b^{q'} \equiv 1 \ (mod\ p)$$

und b nicht irgend einem der a congruent, so hätten wir eine $(q'+1)$te Auflösung der Congruenz $a^{q'} \equiv 1 \ (mod\ p)$, im Widerspruche damit, dass dieselbe nicht mehr als höchstens q' haben kann. Mithin, wenn die q'te Potenz irgend einer Zahl b den Rest 1 lässt, so kann b nicht von allen a verschieden, sondern muss einem derselben congruent sein, d. h. es befindet sich unter den Resten, welche die Potenz x^q möglicher Weise lassen kann.

Hiermit ist folgendes Theorem bewiesen:

Wenn q ein Factor von $p-1$ und

$$q' = \frac{p-1}{q}$$

ist, so können nur solche Zahlen a, welche der Congruenz

$$a^{q'} \equiv 1 \pmod{p}$$

genügen und sonst keine anderen Reste der Potenz x^q sein und alle Zahlen, welche $a^{q'}$ einer von 1 verschiedenen Zahl congruent machen, sind Nichtreste der $q$ten Potenz. Wird die Bedingungscongruenz erfüllt, so hat die Congruenz

$$x^q \equiv a \pmod{p}$$

q von einander verschiedene Wurzeln, welche, wenn m eine derselben und keine der zu q gehörigen Zahlen ist, durch die Reihe der Zahlen

$$m \quad mk \quad mk^2 \quad mk^3 \ldots\ldots mk^{q-1}$$

dargestellt werden.

Nehmen wir unser altes Beispiel wieder auf und untersuchen, ob die Zahlen 8 und 6 Reste oder Nichtreste von x^3 sind; es ist in diesem Falle

$$q = 3, \quad p = 31, \quad q' = 10$$

und man überzeugt sich leicht, dass

$$\left.\begin{array}{l} 8^{10} \equiv 64^5 \equiv (+2)^5 \equiv 1 \\ 6^{10} \equiv 36^5 \equiv 5^5 \equiv 125.25 \equiv -6 \end{array}\right\} \pmod{31}.$$

Mithin ist nach dem Modul 31 die Zahl 8 ein kubischer Rest, dagegen die Zahl 6 ein kubischer Nichtrest.

2) Gehen wir jetzt zu dem allgemeinen Falle über, wenn der Exponent von x eine relative Primzahl zu $p-1$ ist. Sei also die aufzulösende Congruenz

$$x^n \equiv a \pmod{p};$$

so handelt es sich zunächst darum darzuthun, dass überhaupt eine Wurzel derselben existirt. Nun kann man doch zu jeder beliebigen Zahl einen Exponenten auffinden, der ein Divisor von $p-1$ ist und zu welchem diese Zahl gehört. Es möge also der Exponent q zu der Zahl a gehören, so ist

$$a^q \equiv 1 \pmod{p}$$

und der Exponent q auf jeden Fall eine relative Primzahl zu n. Denn da $p-1$ zu n als relative Primzahl gegeben ist, so muss es auch jeder

Factor von $p-1$ sein. Mithin ist es immer möglich, sich die Unbestimmten z und w so zu bestimmen, dass sie die Gleichung

$$nz = qw+1$$

erfüllen. Alsdann folgt, indem man die vorhergehende Congruenz auf die $w$te Potenz erhebt,

$$a^{wq} \equiv 1 \ (mod\ p),$$

und mithin

$$a^{nz} = a^{qw+1} = a^{qw} . a \equiv a \ (mod\ p)$$

oder auch

$$(a^z)^n \equiv (mod\ p),$$

d. h. der Werth

$$x \equiv a^z \ (mod\ p)$$

ist eine Lösung, oder, wie wir in Analogie zu der bei Gleichungen üblichen Ausdrucksweise auch sagen, eine Wurzel der Congruenz

$$x^n \equiv a \ (mod\ p)$$

vom $n$ten Grade.

Wir können aber auch noch weiter gehen und behaupten, dass diese Congruenz überhaupt keine weiteren Lösungen zulässt, als diese eine.

Wäre nämlich eine zweite davon verschiedene Lösung

$$x \equiv s \ (mod\ p)$$

möglich und bestimmte man sich den kleinsten Rest von a^s, so dass

$$a^s \equiv r \ (mod\ p),$$

so müssten zu gleicher Zeit die beiden Congruenzen

$$\left.\begin{array}{l} r^n \equiv a \\ s^n \equiv a \end{array}\right\} (mod\ p)$$

befriedigt werden, aus denen die dritte

$$r^n \equiv s^n \ (mod\ p)$$

fliessen würde. Da nun aber der Annahme zu Folge r und s verschiedene Lösungen, also einander congruent sind, so wird die Auflösung der Congruenz

$$r \equiv sy \ (mod\ p)$$

ein von 1 verschiedenes y ergeben. (Diese Congruenz kann immer bestehen; denn, da a als von 1 und 0 verschieden angenommen werden muss, kann keine der Grössen r und s, welche Lösungen der gegebenen Congruenz sein sollen, weder gleich 1 noch ein Vielfaches von p sein; mithin ist sowohl r wie s eine relative Primzahl zu der Primzahl p.) Setzt man diesen Werth von r in die vorhergehende Congruenz ein, so

bekommt man

$$(zy)^n = z^n y^n \equiv z^n \pmod{p},$$

woher durch Division mit z^n

$$y^n \equiv 1 \pmod{p}.$$

Diese letzte Congruenz kann aber, wie wir wissen, nur dann statthaben, wenn n ein Factor von $p-1$ ist, im Widerspruche zu der Voraussetzung, dass beide relative Primzahlen zu einander sind.

Wir können die Resultate der eben beendigten Untersuchung in folgendes Theorem zusammenfassen:

Wenn n eine relative Primzahl zu $p-1$ und q derjenige Exponent ist, zu welchem die gegebene Zahl a gehört und man bestimmt z vermöge der Congruenz

$$nz \equiv 1 \pmod{q},$$

so ist

$$x \equiv a^z \pmod{p}$$

eine Wurzel der Congruenz

$$x^n \equiv a \pmod{p}$$

und diese Congruenz hat ausser dieser einen keine davon verschiedene Lösung.

Beispiel. Sei die aufzulösende Congruenz

$$x^5 \equiv 3 \pmod{19},$$

also, wie man aus der Tabelle des §. 11 entnehmen oder auch mit leichter Mühe durch Bildung der auf einander folgenden Potenzen von 3 finden kann,

$$q = p - 1 = 18, \quad n = 5:$$

so ergiebt sich zunächst die Hülfscongruenz:

$$5z \equiv 1 \pmod{18}.$$

Die Auflösung derselben, etwa mit Anwendung von Kettenbrüchen, giebt

$$z \equiv -7 \pmod{18}$$

und mithin ist, wenn man den kleinsten positiven Rest, nämlich 11 sich hieraus entnimmt,

$$x \equiv 3^{11} \equiv -9 \equiv 10 \pmod{19}$$

die Lösung der gegebenen Congruenz.

3) Wir kommen endlich auf den letzten noch möglichen Fall, in welchem der Exponent von x zwar nicht unmittelbar ein Theiler von $p-1$ ist, aber doch auch keine relative Primzahl zu $p-1$ ist. Sei also q der

grösste gemeinschaftliche Factor, welchen er mit $p-1$ gemeinschaftlich besitzt, und n eine relative Primzahl zu $p-1$, so ist die vorgelegte Congruenz von der Form

$$x^{nq} \equiv a \ (mod\ p).$$

Da q ein Factor von p ist, so existiren, in der Voraussetzung, dass die gegebene Grösse a der Bedingungscongruenz

$$a^{q'} \equiv 1 \ (mod\ p)$$

Genüge leistet, immer q verschiedene und nach 1) bestimmbare Wurzeln der Congruenz

$$(x^n)^q \equiv a \ (mod\ p).$$

Seien dieselben

$$x^n \equiv y' \ y'' \ y''' \ \ldots\ldots \ y^{(q)} \ (mod\ p),$$

so entspricht, da n und $p-1$ relative Primzahlen sind, jedem y nur ein einziger und zwar nach 2) bestimmbarer Werth von x, so dass

$$x \equiv \xi' \ \xi'' \ \xi''' \ \ldots\ldots \ \xi^{(q)} \ (mod\ p)$$

folgt. Alle diese q Werthe sind von einander verschieden, weil, wenn einige von ihnen einander congruent wären, auch ihre $n$ten Potenzen, d. h. die gleichnamigen y einander congruent wären, im Widerspruche damit, dass dieselben alle als von einander verschieden sich bestimmt haben. Zugleich genügen sie sämmtlich der vorgelegten Congruenz und stellen mithin q verschiedene Wurzeln derselben dar. Mehr können aber überhaupt nicht existiren. Denn gäbe es noch eine Wurzel mehr, welche ein den früheren incongruentes ξ wäre, so könnte man immer ein dazu gehöriges y sich bestimmen, welches der Congruenz

$$\xi^n \equiv y \ (mod\ p)$$

Genüge leistete und von den früheren y verschieden wäre. Dieses y gäbe mithin eine $(q+1)$te Wurzel der Congruenz

$$(x^n)^q \equiv y^q \equiv a \ (mod\ p),$$

da doch höchstens q existiren können. Also sind die vorhergehenden ξ alle nur möglichen von einander verschiedenen Wurzeln, welche unsere Congruenz nur haben kann.

Wenn die Bedingungscongruenz

$$a^{q'} \equiv 1 \ (mod\ p)$$

nicht erfüllt wird, so können überhaupt keine Zahlenwerthe von x angegeben werden, für welche die Potenz x^{nq} die Zahl a zum Rest lassen

könnte. Denn sobald für ein bestimmtes x die Congruenz

$$x^{nq} \equiv a \pmod{p}$$

erfüllt wird, so folgt durch Erhebung auf die Potenz q'

$$x^{nqq'} = x^{n(p-1)} \equiv 1 \equiv a^{q'} \pmod{p},$$

d. h. also wenn a ein Rest der (nq)ten Potenz sein kann, so findet unsere Bedingungscongruenz statt.

Unsere Entwickelung giebt jetzt folgendes Theorem:

Wenn n eine relative Primzahl und q ein Theiler von $p-1$ ist, so hat, wenn die Bedingungscongruenz

$$a^{q'} \equiv 1 \pmod{p}$$

stattfindet, die Congruenz $x^{nq} \equiv a \pmod{p}$, q verschiedene Lösungen, nicht mehr und nicht weniger. Um dieselben zu finden, hat man die beiden Congruenzen

$$\left.\begin{array}{l} y^q \equiv a \\ x^n \equiv y \end{array}\right\} \pmod{p}$$

nach einander aufzulösen.

Beispiel 1. Sei

$$p = 61,\ n = 7,\ a = -13,\ q = 5,\ q' = 12,$$

so ist die aufzulösende Congruenz

$$x^{35} \equiv -13 \pmod{61}$$

und man hat zu Folge der zweiten auf den Modul 61 bezüglichen Tabelle des vorigen Paragraphen

$$-13 \equiv 2^{10} \pmod{61}$$

also

$$(-13)^{q'} \equiv 2^{12 \cdot 10} \equiv 1 \pmod{61},$$

d. h. die Bedingungscongruenz wird erfüllt. Indem wir nun zunächst die Congruenz

$$y^5 \equiv -13 \pmod{61}$$

aufzulösen versuchen, finden wir durch Betrachtung der verschiedenen Reste, welche y^5 für die Zahlen

$$y = 1\ 2\ 3\ \ldots\ldots\ p-1$$

möglicher Weise lassen kann, eine Wurzel

$$y \equiv 4 \pmod{61}.$$

Um alle Wurzeln zu erhalten, nehme man irgend eine der zu dem Exponenten 5 gehörigen Zahlen, etwa die kleinste 9, bilde sich von der Reihe der Potenzen

$$1 \quad 9 \quad 9^2 \quad 9^3 \quad 9^4$$

die Reihe der zugehörigen Reste, nämlich

$$1 \quad 9 \quad 20 \quad -3 \quad -27,$$

und multiplicire alle einzelnen Glieder derselben mit der gefundenen Wurzel 4 (nach dem unter 1) gelehrten Verfahren). Dadurch erhält man die 5 gesuchten Wurzeln wie folgt:

$$y \equiv 4 \quad 36 \quad 80 \quad -12 \quad -108$$

oder, in den kleinsten Zahlen ausgedrückt:

$$y \equiv 4 \quad -25 \quad 19 \quad -12 \quad 14 \pmod{61}.$$

Endlich sind noch die 5 Congruenzen

$$x^7 \equiv 4 \quad -25 \quad 19 \quad -12 \quad 14 \pmod{61}$$

aufzulösen nach der unter 2) angegebenen Methode. Zu dem Zwecke hat man sich zuerst die Exponenten zu bestimmen, zu welchen die Zahlen

$$4 \quad -25 \quad 19 \quad -12 \quad 14$$

gehören; dieselben sind respective

$$30 \quad 30 \quad 30 \quad 30 \quad 6;$$

hierauf müssen die 5 Hilfscongruenzen

$$7z \equiv 1 \pmod{30 \quad 30 \quad 30 \quad 30 \quad 6},$$

die sich indessen hier auf nur 2 von einander verschiedene reduciren, aufgelöst werden. Aus ihnen ergiebt sich:

$$z \equiv \underbrace{13 \quad 13 \quad 13 \quad 13}_{(mod\ 30)} \quad \underbrace{1}_{(mod\ 6)};$$

mithin sind die 5 gesuchten Lösungen der vorgelegten Congruenz

$$x \equiv 4^{13} \quad (-25)^{13} \quad (19)^{13} \quad (-12)^{13} \quad 14^1$$

oder, in den kleinsten Resten ausgedrückt:

$$x \equiv 19 \quad 4 \quad -12 \quad -25 \quad 14 \pmod{61}$$

und diese Resultate sind sehr leicht zu verificiren, da man zu Folge der Anlage der Rechnung

$$-13 \equiv 19^5 \quad 4^5 \quad (-12)^5 \quad (-25)^5 \quad 14^5$$

und

$$1 \equiv 19^{30} \quad 4^{30} \quad (-12)^{30} \quad (-25)^{30} \quad 14^{30}$$

hat.

Beispiel 2. Sei die aufzulösende Gleichung

$$x^{55} \equiv -13 \pmod{61};$$

alsdann hat man

$$p = 61, \quad n = 11, \quad a = -13, \quad q = 5, \quad q' = 12.$$

Indem dieselbe Congruenz 5ten Grades, wie in dem vorigen Beispiele, aufzulösen ist, bleibt alles in der ersten Hälfte der Rechnung, wie vorher; nur die 5 Hilfscongruenzen in z werden andere, nämlich:

$$11z \equiv 1 \ (mod\ 30\ 30\ 30\ 30\ 6)$$

und es ergeben sich daraus für z die in den kleinsten positiven Zahlen ausgedrückten Werthe:

$$z = 11\ 11\ 11\ 11\ 5;$$

mithin sind die 5 Lösungen der vorgelegten Congruenz:

$$x \equiv 4^{11}\ (-25)^{11}\ 19^{11}\ (-12)^{11}\ 14^{5}$$

oder, in den kleinsten Zahlen:

$$x \equiv 5\ -16\ -22\ -15\ -13\ (mod\ 61).$$

Beispiel 3. Es sei

$$p = 31,\ n = 7,\ a = 8,\ q = 3,\ q' = 10;$$

so hat die entsprechende Congruenz die Form

$$x^{21} \equiv 8\ (mod\ 31).$$

Die Auflösung der Congruenz

$$y^{3} \equiv 8\ (mod\ 31)$$

giebt die Wurzeln

$$y = 2\ 10\ 19\ (mod\ 31)$$

und um nun die 3 Congruenzen

$$x^{7} \equiv 2\ 10\ 19\ (mod\ 31)$$

aufzulösen, muss man zunächst die zu den Zahlen 2 10 19 gehörigen Exponenten suchen. Dieselben sind:

$$5\ 15\ 15.$$

Alsdann ist z vermöge der Hilfscongruenzen

$$7z \equiv 1\ (mod\ 5\ 15\ 15)$$

zu bestimmen; man findet leicht:

$$z = 3\ 13\ 13$$

und die Werthe von x in den 3 gesuchten Congruenzen sind nun

$$x \equiv 2^{3}\ 10^{13}\ 13^{13}\ (mod\ 31)$$

oder, in den kleinsten Zahlen:

$$x \equiv 8\ 9\ 14\ (mod\ 31).$$

4) Ein ganz einzelner Fall ordnet sich keinem der betrachteten Hauptfälle unter; es kann nämlich vorkommen, dass eine solche Potenz von x der gegebenen Zahl a congruent werden soll, deren Exponent die Potenz eines Primfactors von $p-1$ ist, ohne jedoch in $p-1$ aufzugehen.

Die Form der Congruenz ist alsdann:

$$x^{c^\varkappa} \equiv a \ (mod\ p)$$

und es ist, wenn $p-1$ den Primfactor c γmal enthält,

$$\varkappa > \gamma,\ q = c^\gamma,\ q' = \frac{p-1}{q}.$$

Wir müssen diesen Fall unabhängig von 1) behandeln und ganz im Allgemeinen die Reste betrachten, welche die Potenz

$$x^{c^\varkappa}$$

nach dem Modul p lassen kann, wenn man für x der Reihe nach die Zahlen

$$1\ 2\ 3\ 4 \ldots\ldots p-1$$

einsetzt.

Suchen wir uns zunächst irgend eine der zu q gehörigen Zahlen k und bilden uns die Reihe der Potenzen:

$$1\ k\ k^2\ k^3 \ldots\ldots k^{q-1},$$

so erhalten wir q Zahlen (nämlich die Reste dieser Potenzen), welche alle untereinander verschieden sind und sämmtlich auf die ($c^\varkappa$)te Potenz erhoben der Einheit congruent werden, wie man sogleich einsieht, wenn man bemerkt, dass k zu q gehört und

$$c^\varkappa = qc^{\varkappa-\gamma}$$

ist. Zu gleicher Zeit sind dieselben auch die einzigen, welche die ($c^\varkappa$)te Potenz von x gleich 1 machen. Dieses beweist sich wie folgt. Wenn andere von den genannten verschiedene Zahlen existirten, die die gleiche Eigenschaft besässen, z. B. l, so würde man haben, wie immer auch n beschaffen sein möge,

$$k^n \text{ incongr. } l$$

und die Zahl l müsste nothwendig zu irgend einem Exponenten gehören, der wegen der Congruenz

$$l^{c^\varkappa} \equiv 1 \ (mod\ p)$$

ein Divisor von $c^\varkappa$ sein müsste, mithin irgend eine Potenz von der Primzahl c. Der Exponent λ dieser Potenz muss nun entweder grösser oder gleich oder kleiner als c^γ sein. Jede dieser drei Annahmen führt aber, wie wir gleich zeigen werden, auf einen Widerspruch. Also ist die Annahme falsch, dass eine von k^n verschiedene Zahl l existiren könne, welche unsere Congruenz befriedigt.

Der Exponent λ kann nicht grösser sein als γ, weil sonst c^λ kein Theiler von $p-1$ sein könnte. Er kann aber auch nicht gleich oder kleiner als γ sein. Denn im ersten Falle wäre unmittelbar

$$l^{c^\gamma} \equiv 1 \ (mod\ p)$$

und im zweiten

$$l^{c^\gamma} = \left(l^{c^\lambda}\right)^{c^{\gamma-\lambda}} \equiv 1^{c^{\gamma-\lambda}}$$

so dass immer noch die vorige Congruenz Bestand haben müsste. In beiden Fällen mithin wäre l eine Wurzel der Congruenz

$$x^{c^\gamma} \equiv 1 \ (mod\ p);$$

dieselbe hat aber, wie wir wissen, die c^γ davon verschiedenen Wurzeln

$$1 \quad k \quad k^2 \quad k^3 \ldots\ldots k^{c^\gamma-1},$$

mithin hätte sie eine Wurzel mehr als sie höchstens haben kann.

Die Zahlen dieser letzten Reihe sind also die einzigen, deren $(c^\varkappa)$te Potenzen den Rest 1 lassen können. Nehmen wir irgend eine davon verschiedene Zahl m, so muss sie mithin einen von 1 verschiedenen Rest r geben, so dass

$$m^{c^\varkappa} \equiv r \ (mod\ p),$$

und die sämmtlichen Zahlen, welche eben denselben Rest r geben, sind alsdann

$$m \quad mk \quad mk^2 \quad mk^3 \ldots\ldots mk^{c^\gamma-1},$$

und alle davon verschiedenen Zahlen geben einen von r verschiedenen Rest.

Um dies Letzte zu zeigen, wollen wir irgend eine Zahl h untersuchen, welcher der Congruenz

$$x^{c^\varkappa} \equiv r \ (mod\ p)$$

Genüge leistet und lösen uns zu dem Zwecke die Congruenz

$$h \equiv m\mu \ (mod\ p)$$

nach μ auf: dann wird folgen, indem man auf beiden Seiten zur $(c^\varkappa)$ten Potenz erhebt,

$$h^{c^\varkappa} \equiv m^{c^\varkappa}\mu^{c^\varkappa}$$

oder, weil sowohl h wie m der vorgelegten Congruenz Genüge thun,

$$1 \equiv \mu^{c^\varkappa} \ (mod\ p);$$

d. h. μ ist eine Wurzel der Congruenz

$$x^{c^\varkappa} \equiv \lambda \ (mod\ p)$$

und muss also nach dem, was wir soeben bewiesen haben, nothwendig

mit irgend einer Potenz von k zusammenfallen; sei diese k^n, so folgt

$$\mu \equiv k^n \ (mod\ p),$$

also durch Multiplication mit m

$$m\mu \equiv mk^n \ (mod\ p)$$

oder endlich, da h und $m\mu$ als congruente Zahlen bestimmt sind,

$$h \equiv mk^n \ (mod\ p),$$

d. h. h muss irgend ein Glied der Reihe

$$m \ mk \ mk^2 \ \ldots\ldots \ mk^{c^\gamma - 1}$$

sein.

Indem man nun irgend eine in der Reihe der Zahlen von 1 bis $p-1$ noch übrig gebliebene Zahl sich auswählt, deren Rest weder 1 noch r sein kann, muss derselbe nothwendig irgend eine von 1 und r verschiedene Zahl r' sein und alle Zahlen, welche diesen Rest r' haben, sind dann in der Reihe

$$m' \ m'k \ m'k^2 \ \ldots\ldots\ldots \ m'k^{c^\gamma - 1}$$

enthalten. Geht man in derselben Weise fort, so sieht man leicht ein, dass man

$$\frac{p-1}{q} = q'$$

Gruppen von je

$$q = c^\gamma$$

Zahlen erhält, so dass von Gruppe zu Gruppe die Potenzreste verschieden, dagegen von den verschiedenen Zahlen einer Gruppe einerlei ausfallen.

Da mithin die $(c^\varkappa)$te Potenz aller aufeinander folgenden Zahlen nur q' verschiedene Reste liefert, so erhellt wiederum, dass die Congruenz

$$x^{c^\varkappa} \equiv a \ (mod\ p)$$

nicht möglich ist, ausser wenn a ein Rest der $(c^\varkappa)$ten Potenz ist. Die Bedingungsgleichung, welche ausdrückt, dass a ein solcher Rest ist, kann leicht gefunden werden. Wenn nämlich eine bestimmte Zahl x existirt, für welche die vorhergehende Congruenz erfüllt wird, so erhält man, indem man auf beiden Seiten zur Potenz q' erhebt,

$$x^{c^\varkappa \cdot q'} = x^{c^{\varkappa - \gamma} q q'} = x^{(p-1) c^{\varkappa - \gamma}} \equiv a^{q'} \ (mod\ p);$$

nun ist aber

$$x^{p-1} \equiv 1,$$

also folgt

$$a^{q'} \equiv 1 \pmod p,$$

d.h. die nämliche Bedingungsgleichung wie in 1).

Nach dem, was wir in dieser Nummer bewiesen haben, können wir folgendes Theorem aufstellen, welches mit dem unter 1) bewiesenen die grösste Aehnlichkeit hat:

a) Wenn c eine Primzahl und c^γ die höchste in $p-1$ enthaltene Potenz dieser Primzahl bedeutet, wenn ferner

$$\gamma < \varkappa$$

ist und der Kürze halber

$$c^\gamma = q, \quad \frac{p-1}{c^\gamma} = q'$$

gesetzt wird, so erhält die Potenz

$$x^{c^\varkappa},$$

wenn man für x nach einander die Zahlen

$$1 \quad 2 \quad 3 \ldots\ldots p-1$$

einsetzt, q' verschiedene Werthe und zwar gehören zu jedem solchen Restwerthe immer q verschiedene Zahlen, durch welche er erzeugt werden kann.

b) Die Congruenz

$$x^{c^\varkappa} \equiv a \pmod p$$

ist nur dann möglich, wenn der Bedingungcongruenz

$$a^{q'} \equiv 1 \pmod p$$

Genüge geschieht, und zwar hat sie, dieses vorausgesetzt, q von einander verschiedene Wurzeln, welche, wenn m eine beliebige darunter und k eine zu dem Exponenten q gehörige Zahl ist, durch die Reihe der Zahlen

$$m \quad mk \quad mk^2 \ldots\ldots mk^{q-1}$$

dargestellt werden.

Beispiel. Die aufzulösende Congruenz sei

$$x^{32} \equiv 25 \pmod{61},$$

also

$$p-1 = 60 = 2^2.3.5, \quad c^\gamma = q = 4, \quad q' = 15, \quad c^\varkappa = 2^5 = 32.$$

Die Bedingungscongruenz

$$25^{15} \equiv 1 \pmod{61}$$

wird erfüllt; denn man hat

$25^2 \equiv 15, 25^3 \equiv 9, 25^4 \equiv -19, 25^7 \equiv 12, 25^8 \equiv -5, 25^{15} = 25^7 . 25^8 \equiv -60 \equiv 1.$
Eine Wurzel findet sich leicht durch Probiren, nämlich 5; in der That ist, wie wir oben sahen,

$$25^8 = 5^{16} \equiv -5 \ (mod\ 61),$$

mithin durch Quadrirung auf beiden Seiten

$$5^{32} \equiv 25.$$

Sucht man sich jetzt irgend eine der zu dem Exponenten 4 gehörigen Zahlen, etwa 11, so sind die sämmtlichen 4 Wurzeln unserer Congruenz:

$$5 \quad 5.11 \quad 5.11^2 \quad 5.11^3$$

oder, wenn man die kleinsten Reste nimmt:

$$5 \quad -6 \quad -5 \quad 6,$$

(55) (56)

5) Die sämmtlichen Theoreme, welche den Inhalt dieses Paragraphen bilden, lassen sich nach ihrem hauptsächlichsten Inhalte in folgende beiden Theoreme zusammenziehen:

a) Die Congruenz

$$x^n \equiv a \ (mod\ p)$$

hat, wenn a ein Rest der $n$ten Potenz sein kann, soviele Lösungen als der grösste gemeinsame Theiler q zwischen n und $p-1$ Einheiten hat, und die Grösse a ist ein Rest oder Nichtrest der $n$ten Potenz, je nachdem die Bildungscongruenz

$$a^{q'} \equiv 1 \ (mod\ p), \ q' = \frac{p-1}{q}$$

erfüllt oder nicht erfüllt wird.

b) Die Substitution der Zahlen

$$1 \ 2 \ 3 \ 4 \ldots\ldots p-1$$

für x in den Ausdruck x^n giebt q' verschiedene Reste der $n$ten Potenz und so zwar, dass zu jedem einzelnen Reste q verschiedene Zahlenwerthe von x gehören.

Wenn $q=1$, d. h. n und $p-1$ relative Primzahlen sind, so folgt hieraus, dass die Reste der Potenzen x^n, welche durch die Substitution der Zahlen 1, 2, 3, ... $p-1$ erhalten werden, alle untereinander verschieden sind. Es entstehen dann nämlich $p-1$ Gruppen, jede zu einer Zahl, und wir können daher folgendes speciellere, auf diesen Fall bezügliche Theorem aussprechen:

c) Wenn n eine relative Primzahl zu $p-1$ ist, so sind die Reste der Potenzen

$$1\ 2^n\ 3^n\ 4^n \ldots\ldots (p-1)^n$$

alle von einander verschieden und kommen daher, abgesehen von der Reihenfolge, mit der Reihe der Zahlen

$$1\ 2\ 3\ 4\ 5 \ldots . p-1$$

überein.

Es wird nicht überflüssig sein zu bemerken, dass, wenn in der Congruenz

$$x^n \equiv a \ (mod\ p)$$

der Exponent n grösser als der Modul p sein sollte, dieselbe durch eine Congruenz von geringerem Grade ersetzt werden kann, nämlich durch die Congruenz

$$x^\nu \equiv a \ (mod\ p)$$

in welcher ν den kleinsten positiven Rest von n nach dem Modul $p-1$ bezeichnet. Es ist nämlich alsdann n von der Form

$$n = b(p-1)+\nu,$$

mithin

$$x^n = x^{b(p-1+\nu} = (x^{p-1})^b . x^\nu$$

oder, da nach Fermat's Satze

$$x^{p-1} \equiv 1$$

ist,

$$x^n \equiv x^\nu \ (mod\ p),$$

so dass jeder Zahlenwerth für x, der die Potenz x^n gleich a macht, auch die niedrigere Potenz x^ν gleich a machen muss. Beide Congruenzen sonach, sowohl die, welche sich auf die $n$te Potenz, wie die, welche sich auf die νte bezieht, haben dieselben Wurzeln.

Uebrigens lässt sich die eben gemachte Bemerkung verallgemeinern, und man hat, wenn der Grad einer beliebig zusammengesetzten Congruenz eine höhere Zahl, als der Modul und der Modul eine Primzahl p ist, dieselbe immer als identisch mit einer Congruenz von niedrigerem Grade, welche dadurch aus der gegebenen abgeleitet wird, dass man überall die Exponenten der Unbestimmten x durch andere ersetzt, welche die kleinsten positiven Reste der früheren in Bezug auf den Modul $p-1$ sind.

Dies vorausgesetzt erhellt, dass, wie der Exponent n der Congruenz

$$x^n \equiv a \pmod{p}$$

auch beschaffen sein möge, die Auflösung schliesslich immer auf die Untersuchung einer solchen Congruenz

$$x^q \equiv b \pmod{p}$$

zurückführt, in welcher der Exponent q ein Theiler von $p-1$ ist. Diese letzte Congruenz setzt, wie wir wissen, zu ihrer vollständigen Lösung die Kenntniss wenigstens einer Wurzel voraus, vermöge welcher, wenn ausserdem die zu q gehörigen Zahlen bekannt sind, die übrigen ohne Schwierigkeit ausgedrückt werden können; aber diese Wurzel kann im Allgemeinen nur durch Probiren bestimmt werden. Demgemäss sind, um leicht und ohne ermüdende Rechnungen in jedem einzelnen Falle zum Ziele zu gelangen, durchaus Tabellen erforderlich, welche sich auf die verschiedenen Theiler einer Primzahl beziehen, die dazu gehörigen Zahlen enthalten und ausserdem wenigstens eine Wurzel irgend einer auf einen solchen Theiler bezüglichen Congruenz. Diese Tabellen indessen, deren Berechnung ein ziemlich weitläufiges Geschäft ist, werden entbehrlich, wenn man die in §. 12 angedeuteten beiden Tabellen besitzt. Vermittelst der letzteren ist man nämlich im Stande, sich die Wurzeln einer beliebigen Congruenz mit Leichtigkeit zu bestimmen. Wir begnügen uns, an ein paar Beispielen das Verfahren anzudeuten und alles die Theorie über den Gebrauch solcher Tafeln betreffende Detail zu übergehen.

Sei zuerst die Congruenz

$$x^{32} \equiv 9 \pmod{61}$$

aufzulösen. Dieselbe verwandelt sich zu Folge der Substitutionen

$$x \equiv 2^{\xi},\ 9 \equiv 2^{12} \pmod{61}$$

in

$$2^{32\xi} \equiv 2^{12} \pmod{61},$$

welche zu Folge der Periodicität, die zwischen den aufeinander folgenden Potenzen einer primitiven Wurzel eintritt, nicht anders bestehen kann, als wenn

$$32\xi \equiv 12 \pmod{60}$$

ist. Diese letzte Congruenz geht durch Division mit 4 über in die Congruenz

$$8\xi \equiv 3 \pmod{15},$$

welcher durch

$$\xi \equiv 6 \ (mod\ 15)$$

Genüge geschieht. Bilden wir uns alle Werthe von ξ, die nach dem Modul 61 verschieden sind, so sind es folgende 4:

$$\xi = 6 \quad 21 \quad 36 \quad 51$$

und man bekommt daher für x die 4 Werthe:

$$x \equiv 2^6 \quad 2^{21} \quad 2^{36} \quad 2^{51}$$

oder zu Folge der Tabelle

$$x \equiv 3 \quad -28 \quad -3 \quad 28 \ (mod\ 61).$$

Dies sind die 4 Wurzeln, welche überhaupt möglich sind.

Beispiel 2. Sei die aufzulösende Congruenz

$$x^{32} \equiv -9 \ (mod\ 61);$$

dieselbe geht durch die Substitutionen

$$x \equiv 2^{\xi}, \ -9 \equiv 2^{42}$$

über in die folgende

$$2^{32\xi} \equiv 2^{42} \ (mod\ 61)$$

und damit diese bestehen könne, muss

$$32\xi \equiv 42 \ (mod\ 60)$$

oder einfacher

$$16\xi \equiv 21 \ (mod\ 30)$$

sein. Diese letztere Congruenz ist aber offenbar unmöglich, weil 16 mit dem Modul 30 den gemeinschaftlichen Factor 2 besitzt, ohne dass dieser auch in die andere Seite der Congruenz ohne Rest aufgehe. Also ist auch die vorgelegte Congruenz unmöglich oder mit andern Worten -9 ist ein Nichtrest der 9ten Potenz. In der That ist es leicht sich zu überzeugen, dass $(-9)^{15}$ der Congruenz 1 nicht genügt.

Beispiel 3. Sei die aufzulösende Congruenz

$$x^{37} \equiv -27 \ (mod\ 61);$$

vermöge der Werthe

$$x \equiv 2^{\xi}, \ -27 \equiv 2^{48}$$

wird

$$2^{37\xi} \equiv 2^{48} \ (mod\ 61),$$

woher

$$37\xi \equiv 48 \ (mod\ 60).$$

Die Anwendung von Kettenbrüchen giebt folgende Rechnung:

	1	1	1	1	1	1	4
$\frac{0}{1}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{3}{5}$	$\frac{5}{8}$	$\frac{8}{13}$	

und man findet leicht, dass 37ξ für $\xi = 13$ congruent 1 wird, mithin wird es für

$$\xi = 48.13 \equiv 24 \ (mod\ 60)$$

congruent 48; zugleich sieht man, dass von allen Zahlen zwischen 0 und 61 24 der einzige mögliche Werth von ξ ist, also folgt

$$\xi = 24$$

und hieraus

$$2^{\xi} = x \equiv 20 \ (mod\ 61),$$

die einzige Auflösung, deren die vorgelegte Congruenz fähig ist.

Beispiel 4. Die gegebene Congruenz sei

$$x^{35} \equiv 29 \ (mod\ 61);$$

man transformirt dieselbe ohne Schwierigkeit in die folgende:

$$2^{35\xi} \equiv 2^{35} \ (mod\ 61),$$

aus der man wieder

$$35\xi \equiv 35 \ (mod\ 60)$$

schliesst. Hieraus wird zunächst

$$7\xi \equiv 7 \ (mod\ 12)$$

und, da 7 und 12 relative Primzahlen sind,

$$\xi \equiv 1 \ (mod\ 12).$$

Diejenigen Werthe von ξ zwischen 0 und 61 (die also nach dem Modul 61 von einander verschieden sind), welche dieser Congruenz genügen, sind

$$\xi = 1 \quad 13 \quad 25 \quad 37 \quad 49$$

und hieraus erhält man für x die Potenzwerthe

$$2^{1} \quad 2^{13} \quad 2^{25} \quad 2^{37} \quad 2^{49},$$

oder, wenn man die in der Tabelle verzeichneten kleinsten Reste nimmt:

$$x \equiv 2 \quad 18 \quad -21 \quad -6 \quad 7 \ (mod\ 61)$$

und in der That hat die untersuchte Congruenz, da 5 der grösste gemeinsame Theiler zwischen 35 und 60 ist, nicht mehr als 5 von einander verschiedene Wurzeln.

Zum Schlusse mögen noch, um dem Anfänger ein angemessenes Material zu bieten, aus dem er sich Beispiele zur Uebung entnehmen mag, die Perioden der Reste folgen, welche für den Modul 61 entstehen, wenn man die Glieder der Zahlenreihe

$$1 \ 2 \ 3 \ 4 \ldots\ldots p-1$$

auf die 10 ersten und noch einige andere Potenzen erhebt, namentlich zu allen solchen, deren Exponenten Theiler von $p-1=60$ sind. Es

möchte dies um so weniger überflüssig sein, als die Betrachtung einzelner Perioden zu allerlei Inductionen führen kann, welche mit interessanten Sätzen zusammenhängen.

$x^2 \equiv r \pmod{61}$.

r	x	r	x	r	x	r	x	r	x
1	1 —1	13	14 —14	21	12 —12	—5	19 —19	—16	17 —17
3	8 —8	14	21 —21	25	5 —5	—9	28 —28	—19	15 —15
4	2 —2	15	25 —25	27	24 —24	—12	7 —7	—20	23 —23
5	26 —26	16	4 —4	—1	11 —11	—13	29 —29	—22	10 —10
9	3 —3	19	18 —18	—3	27 —27	—14	13 —13	—25	6 —6
12	16 —16	20	9 —9	—4	22 —22	—15	30 —30	—27	20 —20

$x^3 \equiv r \pmod{61}$.

r	x	r	x	r	x
1	1 13 —14	24	8 10 —18	—20	27 —15 —12
3	4 5 —9	27	3 19 —22	—11	11 21 29
8	2 26 —28	28	23 —17 —6	—9	—25 —20 —16
9	16 20 25	—28	6 17 —23	—8	28 —26 —2
11	—29 —21 —11	—27	22 —19 —3	—3	9 —5 —4
20	12 15 —27	—24	18 —10 —8	—1	14 —13 —1
23	—30 —24 —7	—23	7 24 30		

$x^4 \equiv r \pmod{61}$.

r	x	r	x	r	x
1	1 11 —1 —11	16	2 22 —22 —2	—19	25 30 —30 —25
9	8 27 —27 —8	20	3 28 —28 —3	—14	14 29 —29 —14
12	4 17 —17 —4	22	7 16 —16 —7	—5	15 18 —18 —15
13	13 21 —21 —13	25	19 26 —26 —19	—4	10 12 —12 —10
15	5 6 —6 —5	—27	9 23 —23 —9	—3	20 24 —24 —20

$x^5 \equiv r \pmod{61}$.

r	x	r	x
1	1 9 20 —27 —8	—29	2 7 18 21 6
11	8 11 28 —24 —23	—21	26 30 —29 —17 —10
13	12 25 —19 —14 —4	—14	13 15 16 22 —5
14	5 —22 —16 —15 —13	—13	4 14 19 —25 —12
21	10 17 29 —30 —26	—11	23 24 —28 —11 —8
29	6 21 —18 —7 —2	—1	3 27 —20 —9 —1

$x^6 \equiv r \ (mod\ 61).$

r	x						r	x					
1	1	13	14	−14	−13	−1	−27	12	15	27	−27	−15	−12
3	2	26	28	−28	−26	−2	−20	7	24	30	−30	−24	−7
9	4	5	9	−9	−5	−4	−9	6	17	23	−23	−17	−6
20	16	20	25	−25	−20	−16	−3	3	19	22	−22	−19	−3
27	8	10	18	−18	−10	−8	−1	11	21	29	−29	−21	−11

$x^{10} \equiv r \ (mod\ 61).$

r	x									
1	1	3	9	20	27	−27	−20	−9	−3	−1
13	5	13	15	16	22	−22	−16	−15	−13	−5
14	10	17	26	29	30	−30	−29	−26	−17	−10
−14	4	12	14	19	25	−25	−19	−14	−12	−4
−13	2	6	7	18	21	−21	−18	−7	−6	−2
−1	8	11	23	24	28	−28	−24	−23	−11	−8

$x^{12} \equiv r \ (mod\ 61).$

r	x											
1	1	11	13	14	21	29	−29	−21	−14	−13	−11	−1
9	2	3	19	22	26	28	−28	−26	−22	−19	−3	−2
20	4	5	6	9	17	23	−23	−17	−9	−6	−5	−4
−27	7	16	20	24	25	30	−30	−25	−24	−20	−16	−7
−3	8	10	12	15	18	27	−27	−18	−15	−12	−10	−8

$x^{15} \equiv r \ (mod\ 61).$

r	x														
1	1	9	12	13	15	16	20	22	25	−27	−19	−14	−5	−4	−3
11	2	7	18	23	24	26	30	−29	−28	−21	−16	−11	−10	−8	−6
−11	6	8	10	11	17	21	28	29	−30	−26	−24	−23	−18	−7	−2
−1	3	4	5	14	19	27	−25	−22	−20	−16	−15	−13	−12	−9	−1

$x^{30} \equiv r \ (mod\ 61).$

r	x														
+1	±1	±3	±4	±5	±9	±12	±13	±14	±15	±16	±19	±20	±22	±25	±27
−1	±2	±6	±7	±8	±10	±11	±17	±18	±21	±23	±24	±26	±28	±29	±30

$x^7 \equiv r \pmod{61}$.

r	x	r	x	r	x	r	x	r	x	r	x
1	1	11	−11	21	−21	−30	−17	−20	−9	−10	−30
2	−18	12	25	22	15	−29	29	−19	12	−9	3
3	27	13	13	23	28	−28	8	−18	7	−8	−24
4	19	14	14	24	−23	−27	20	−17	−26	−7	−6
5	22	15	16	25	−4	−26	−10	−16	−5	−6	−2
6	2	16	5	26	10	−25	4	−15	−16	−5	−22
7	6	17	26	27	−20	−24	23	−14	−14	−4	−19
8	24	18	−7	28	−8	−23	−28	−13	−13	−3	−27
9	−3	19	−12	29	−29	−22	−15	−12	−25	−2	18
10	30	20	9	30	17	−21	21	−11	11	−1	−1

$x^8 \equiv r \pmod{61}$.

r	x				r	x				r	x			
1	1	11	−11	−1	16	10	12	−12	−10	−19	5	6	−6	−5
9	20	24	−24	−20	20	8	27	−27	−8	−14	13	21	−21	−13
12	2	22	−22	−2	22	4	17	−17	−4	−5	25	30	−30	−25
13	14	29	−29	−14	25	15	18	−18	−15	−4	7	16	−16	−7
15	19	26	−26	−19	−27	3	28	−28	−3	−3	9	23	−23	−9

$x^9 \equiv r \pmod{61}$.

r	x			r	x			r	x		
1	1	13	−14	24	2	26	−28	−20	3	19	−22
3	−25	−20	−16	27	4	5	−9	−11	−29	−21	−11
8	6	17	−23	28	−30	−24	−7	−9	27	−15	−12
9	12	15	−27	−28	7	24	30	−8	23	−17	−6
11	11	21	29	−27	9	−5	−4	−3	16	20	25
20	22	−19	−3	−24	28	−26	−2	−1	14	−13	−1
23	18	−10	−8	−23	8	10	−18				

$x^{35} \equiv r \pmod{61}$.

r	x					r	x				
1	1	9	20	−27	−3	−29	6	21	−18	−7	−2
11	23	24	−28	−11	−8	−21	10	17	29	−30	−26
13	12	25	−19	−14	−4	−14	13	15	16	22	−5
14	5	−22	−16	−15	−13	−13	4	14	19	−25	−12
21	26	30	−29	−17	−10	−11	8	11	28	−24	−23
29	2	7	18	−21	−6	−1	3	27	−20	−9	−1

Von den vielen Theoremen, auf welche eine Durchsicht der vorigen Tabelle führt, wollen wir wenigstens eins anmerken, dass nämlich, wenn q der grösste gemeinschaftliche Theiler zwischen $p-1$ und dem Expo-

nenten n der betrachteten Potenz von x ist, die auf die $q$te Potenz bezügliche Periode aus den nämlichen Restzahlen besteht, aus denen die auf die $n$te Potenz bezügliche Periode sich zusammensetzt, sowie dass, wenn man im ersten Falle die auf ein specielles r bezüglichen q Zahlenwerthe von x betrachtet, im zweiten Falle immer ein specielles und im Allgemeinen von jenem verschiedenes r aufgefunden werden kann, welchem genau dieselben Zahlenwerthe von x zugehören. Wir werden später Gelegenheit nehmen die Betrachtung dieser Restperioden von einem allgemeineren Gesichtspuncte aus wieder aufzunehmen.

§. 14.

Theorie der Congruenz $x^N \equiv r \pmod{P}$, wenn der Modul P eine irgendwie zusammengesetzte Zahl ist.

1) Bis jetzt haben wir überall die Voraussetzung gemacht, dass der Modul p eine Primzahl ist und es entsteht daher die Frage, wie sich die Theorie der Congruenz

$$x^n \equiv 1 \pmod{P}$$

gestalten werde, wenn P nicht mehr eine Primzahl, sondern irgend welche zusammengesetzte Zahl, etwa

$$P = a^\alpha b^\beta c^\gamma \ldots,$$

bezeichnet.

Die Untersuchung nimmt ihren Ausgangspunct naturgemäss von Fermat's Theoreme, dessen Verallgemeinerung wir in einem früheren Paragraphen bewiesen haben und welches also lautet:

Wenn P eine irgendwie zusammengesetzte Zahl und

$$\pi = S'''P = a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \ldots (a-1)(b-1)(c-1) \ldots$$

die Anzahl der Zahlen bedeutet, welche kleiner als P und relative Primzahlen zu P sind, so ist die Congruenz

$$x^\pi \equiv 1 \pmod{P}$$

für jeden Werth von x gültig, der mit dem Modul P keinen gemeinschaftlichen Factor besitzt.

Wir werden im Nachfolgenden unter x immer eine Zahl von der eben bezeichneten Art (und natürlich kleiner als P; denn wäre sie grösser

als P, so müsste sie irgend einer relativen Primzahl zu P, die kleiner als diese Zahl ist, congruent sein und könnte ohne Weiteres mit dieser vertauscht werden) verstehen und diese Beschränkung rechtfertigt sich ganz von selbst, da ohne sie unsere Congruenz überhaupt keinen ordentlichen Sinn hat. Denn wenn x und P einen gemeinschaftlichen Factor hätten, so könnte man aus ihr folgern

$$x^{\pi} \equiv 1 \ (mod\ m),$$

welches widersinnig ist, da die linke Seite den Rest 0 giebt.

Wir entnehmen aus dem Vorhergehenden noch unmittelbar folgende Sätze und Erklärungen:

Wenn für irgend ein bestimmtes x die Congruenz

$$x^{q} \equiv 1 \ (mod\ P)$$

erfüllt wird und zu gleicher Zeit x^{q} die niedrigste Potenz von x ist, welche der Einheit congruent wird, so sagt man; die Zahl x gehört zu dem Exponenten q und dieser Exponent q ist immer ein Theiler von

$$\pi = S'''P,$$

sowie von jedem Exponenten n, für welchen man

$$x^{n} \equiv 1 \ (mod\ P)$$

hat.

Wenn die Congruenz

$$x^{\pi} \equiv 1 \ (mod\ P)$$

für irgend ein bestimmtes x und für keinen niedrigeren Exponenten als π besteht, so nennt man die Zahl x eine primitive Wurzel des Moduls P. Die primitive Wurzel von P ist mithin eine solche Zahl, welche zu dem Exponenten π gehört.

Wenn eine Zahl x existirt, die zu dem Exponenten q gehört, so sind die Reste der Potenzen

$$1 \quad x \quad x^{2} \ \ldots\ldots \ x^{q-1}$$

nach dem Modul p alle von einander verschieden; sie fallen mithin für den Fall, dass x eine primitive Wurzel bezeichnet, d. h. wenn $q = \pi$ ist, mit der Reihe der Zahlen zusammen:

$$1 \quad m' \quad m'' \quad m''' \ \ldots\ldots \ \pi - 1,$$

welche kleiner als P und relative Primzahlen zu P sind.

2) Wir gehen jetzt, um mit der Betrachtung des Einfacheren zu beginnen, zu dem speciellen Falle über, in welchem der Modul P die Potenz irgend einer Primzahl, also von der Form

$$P = p^n$$

ist. Die Grösse P wird in diesem Falle

$$\pi = S'''p^n = (p-1)p^{n-1};$$

die primitiven Wurzeln, wenn es deren giebt, gehören also zu dem Exponenten $(p-1)p^{n-1}$ und wenn zu den übrigen Zahlen zwischen 1 und P, die relative Primzahlen zu P sind, irgend welche Exponenten gehören — und das ist unbedingt nothwendig; denn die πte Potenz einer solchen Zahl giebt 1, also, wenn die πte Potenz nicht die niedrigste ist, welche diesen Rest lässt, so muss es irgend eine andere noch niedrigere Potenz geben, welche die genannte Eigenschaft gleichfalls besitzt — so müssen dieselben Divisoren von π, also, wenn man unter q einen Theiler von $p-1$ und unter λ eine Zahl versteht, die nicht über $n-1$ sein darf, nothwendig die Form

$$qp^\lambda$$

haben. Um nun die Frage zu erledigen, ob wirklich zu jedem solchen Divisor ein oder mehrere Zahlen nach dem Modul P gehören, schicken wir folgende einleitende Sätze voraus:

a) Wenn die Differenz

$$x^{qp^\varkappa} - 1$$

durch die $n$te und keine höhere Potenz von p theilbar ist, so ist auch die Differenz

$$x^{qp^{\varkappa+\lambda}} - 1$$

durch die $(n+\lambda)$te und keine höhere Potenz von p ohne Rest theilbar.

Wir beweisen den Satz zunächst für den speciellen Fall $\lambda = 1$.

Zu Folge der Voraussetzung ist

$$x^{qp^\varkappa} = 1 + Xp^n$$

und zwar hierin X auf keinen Fall durch p theilbar, weil sonst p^n nicht die höchste in unsere Differenz aufgehende Potenz wäre; wir erhalten durch Erhebung dieser Gleichung auf die $p$te Potenz

$$\left(x^{qp^\varkappa}\right)^p = 1 + pXp^n + p\frac{p-1}{2}X^2p^{2n} + \ldots.$$

oder

$$x^{qp^{x}+1}-1 = Xp^{n+1}+\frac{p-1}{2}X^{2}p^{2n+1}+\frac{p-1}{2}\,\frac{p-2}{3}X^{3}p^{3n+1}+\ldots\ldots$$
$$+X^{p-1}p^{(p-1)n+1}+X^{p}p^{pn}.$$

Die rechte Seite dieser Gleichung ist eine Reihe mit lauter ganzzahligen Coefficienten. Denn der allgemeine Ausdruck für die Binomialcoefficienten der $p$ten Potenz

$$\frac{p}{1}\cdot\frac{p-1}{2}\cdot\frac{p-1}{3}\ldots\ldots\ldots\ldots\frac{p-\overline{h-1}}{h}$$

ist immer eine ganze Zahl; mithin wenn p eine ungerade Primzahl und daher zu allen Factoren des Nenners eine relative Primzahl ist, ist es der Ausdruck

$$\frac{p-1}{2}\cdot\frac{p-2}{3}\ldots\ldots\frac{p-\overline{h-1}}{h}$$

gleichfalls, mit einziger Ausnahme des Falles $h = p$, der dem letzten Gliede unserer Reihe entspricht und übrigens von uns auch hier nicht in Anspruch genommen zu werden braucht. Dies vorausgesetzt sieht man sogleich ein, dass sämmtliche Glieder, die auf das erste folgen, höhere Potenzen von p enthalten, als die $(n+1)$te, die im ersten Gliede vorkommt; ausgenommen ist nur der Fall $p = 1$, welcher nicht in Betracht kommen kann. Mithin ist die ganze rechte Seite und folgeweise auch der Ausdruck links durch p^{n+1} theilbar, aber nicht durch irgend eine höhere Potenz von p. Denn dies würde die Theilbarkeit durch p^{n+2} voraussetzen, während doch bei der Division mit dieser Grösse, da X eine relative Primzahl zu p ist, nothwendig ein Rest bleiben muss.

Wenn p der geraden Primzahl 2 gleich ist, so reducirt sich die obige Reihe auf ihr erstes und letztes Glied und es haben genau die nämlichen Schlussfolgerungen statt, wie wenn p ungerade ist, mit einziger Ausnahme des Falles $n = 1$. Denn alsdann erhalten wir

$$x^{qp^{x}+1}-1 = p^{2}(X+X^{2})$$

und es wird jedes Mal die rechte Seite durch eine höhere Potenz von $p = 2$, als die zweite theilbar sein müssen und in gleicher Weise daher auch die linke, d. h. die betrachtete Differenz.

Z. B. Es ist

$$7^{1} \equiv 1 \ (mod\ 2)$$

und offenbar die Differenz $7-1$ durch keine höhere Potenz von 2 als die erste theilbar.

Bildet man sich hieraus die Congruenz $7^1 . 2^1 \equiv 1 \ (mod\ 2^{1+1})$ oder

$$7^2 \equiv 1 \ (mod\ 4),$$

so wird dieselbe allerdings befriedigt, aber sie wird zu gleicher Zeit auch durch den Modul $16 = 2^4$ befriedigt, so dass man

$$7^2 \equiv 1 \ (mod\ 16)$$

hat, in dem Sinne, dass die 4te Potenz von 2 die höchste ist, welche die Differenz $7^2 - 1$ theilt. Wir wollen, um anzudeuten, dass eine Congruenz in Bezug auf ihren Modul der eben bezeichneten Nebenbedingung unterworfen ist, den Modul in Doppelklammern einschliessen und werden die vorhergehende Congruenz dann kurz wie folgt schreiben können:

$$7^2 \equiv 1 \ ((mod\ 2^4)).$$

Aus ihr folgt also, wie bewiesen, indem wir ebensowohl den Exponenten von 2^1, wie den des Moduls um 1 erhöhen,

$$7^4 = 7^{2^2} \equiv 1 \ ((mod\ 2^5))$$

und in der That giebt $7^4 - 1 = 2400$ durch $32 = 2^5$ dividirt die ungerade Zahl 75, d. h. es ist durch keine höhere Potenz von 2 theilbar als die 5te.

Also abgesehen von dem Ausnahmefalle

$$p = 2, \ n = 1$$

gilt ganz allgemein der Satz, dass aus der Congruenz

$$x^{qp^{\varkappa}} \equiv 1 \ ((mod\ p^n))$$

die Congruenz

$$x^{qp^{\varkappa+1}} \equiv 1 \ ((mod\ p^{n+1}))$$

folgt. Indem man diesen Satz zu wiederholten Malen anwendet, folgert man allmählig:

$$x^{qp^{\varkappa+2}} \equiv 1 \ ((mod\ p^{n+2})),$$

$$x^{qp^{\varkappa+3}} \equiv 1 \ ((mod\ p^{n+3})),$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$x^{qp^{\varkappa+\lambda}} \equiv 1 \ ((mod\ p^{n+\lambda})),$$

d. h. der Satz gilt in der von uns ausgesprochenen Allgemeinheit.

Beispiele.

$$8^2 = 64 \equiv 1 \ ((mod\ 3^2)),$$

$$8^{2 . 3^1} = 8^6 = 262144 \equiv 1 \ ((mod\ 3^3)),$$

$$8^{2 . 3^2} = 8^{18} = 2^{54} \equiv 1 \ ((mod\ 3^4)).$$

Um die letzte Congruenz zu verificiren bemerke man, dass nach Köhler's logarithmisch-trigonometrischem Handbuche

$$2^{27} = 134217728$$

und mithin

$$2^{54} - 1 = 134217729 \, . \, 134217727.$$

Der zweite Factor dieses Productes ist durch 3 überhaupt nicht theilbar; der erste giebt durch $3^4 = 81$ dividirt den Quotienten

$$1657009,$$

welcher gleichfalls durch 3 sich nicht weiter theilen lässt.

b) Umkehrung des vorigen Satzes.

Wenn die Differenz

$$x^{qp^x} - 1$$

durch die *n*te und keine höhere Potenz der Primzahl *p* theilbar ist, so ist, in der Voraussetzung, dass die Ungleichungen

$$\lambda < n, \; \lambda \leqq x$$

bestehen, die Differenz

$$x^{qp^{x-\lambda}} - 1$$

durch die $(n - \lambda)$te und keine höhere Potenz von *x* theilbar.

Die Ungleichungen, welche in diesem Satze auftreten, haben den Sinn zu verhüten, dass der Exponent von *x* oder auch der in dem Modul vorkommende negative ausfalle, weil in diesem Falle unsere Congruenzen keine ordentliche Bedeutung mehr haben.

Zunächst ist ersichtlich, dass man

$$x^{qp^{x-\lambda}} \equiv 1 \; (mod \; p)$$

hat; denn wäre

$$x^{qp^{x-\lambda}} \equiv a \; (mod \; p)$$

und hierbei *a* von 1 verschieden, so würde durch Erhebung auf die Potenz p^λ folgen:

$$x^{qp^x} \equiv a^{p^\lambda} \; (mod \; p).$$

Die linke Seite dieser Congruenz giebt zu Folge der Voraussetzung 1, die rechte giebt nach Fermat's Satze

$$a^{p^\lambda} = (a^{p-1} . a)^{p^{\lambda-1}} \equiv a^{p^{\lambda-1}} \equiv a^{p^{\lambda-2}} \equiv \ldots\ldots \equiv a^p \equiv a;$$

mithin würde die widersinnige Congruenz

$$1 \equiv a \; (mod \; p)$$

folgen.

Um jetzt die höchste Potenz von p zu bestimmen, welche in die Differenz

$$x^{qp^{\varkappa-\lambda}}-1$$

aufgeht, setzen wir dieselbe für den Augenblick gleich $p^{\lambda'}$; es hat alsdann die Congruenz

$$x^{qp^{\varkappa-\lambda}} \equiv 1 \ ((mod\ p^{\lambda'}))$$

statt, aus der nach a) sich sogleich die neue

$$x^{qp^{\varkappa}} \equiv 1 \ ((mod\ p^{\lambda+\lambda'}))$$

ergiebt. Zu Folge der Voraussetzung ist mithin

$$n=\lambda+\lambda', \text{ also } \lambda'=n-\lambda,$$

worin unser Satz liegt.

Beispiel. Zu Folge des letzten Beispieles zu a) hat man

$$4^{3^3}=4^{27}=(134217728)^2 \equiv 1 \ ((mod\ 3^{14}));$$

nach unserm Satze folgt hieraus

$$4^3 \equiv 1 \ ((mod\ 3^2))$$

und hieraus

$$4^1 \equiv 1 \ ((mod\ 3))$$

und beide Congruenzen lassen sich mit Leichtigkeit verificiren.

c) Wenn eine Zahl x zu irgend einem Exponenten $qp\lambda$ nach dem Modul p^n gehört, so ist immer, vorausgesetzt, dass λ von 0 verschieden,

$$x^{qp^{\lambda}} \equiv 1 \ ((mod\ p^n))$$

oder die Differenz

$$x^{qp^{\lambda}}-1$$

durch keine höhere Potenz von p als die $n$te theilbar.

Setzen wir den vorläufig noch unbekannten Exponenten der höchsten Potenz von p, welche unserer Congruenz genügt, gleich $n+\varepsilon$, so haben wir

$$x^{qp^{\lambda}} \equiv 1 \ ((mod\ p^{n+\varepsilon}))$$

und die Grösse ε entweder grösser oder kleiner oder gleich λ. Nun kann sie weder grösser, noch gleich sein; denn in beiden Fällen würde gemäss b) folgen:

$$x^{q} \equiv 1 \ ((mod\ p^{n+\varepsilon-\lambda})),$$

also, da $n+\varepsilon-\lambda$ für beide Annahmen nicht unter n betragen kann, jedenfalls

$$x^{q} \equiv 1 \ (mod\ p^n)$$

und es müsste, da x nach der Voraussetzung zu dem Exponenten qp^λ gehört, q ein Multiplum von qp^λ sein, was nicht anders angeht, als wenn $\lambda = 0$ ist, ein Fall, den wir ausdrücklich ausgeschlossen haben. Mithin ist ε nothwendig kleiner als λ und dieses vorausgesetzt giebt die Anwendung von b)

$$x^{qp^{\lambda-\varepsilon}} \equiv 1 \ ((mod\ p^n));$$

es muss also, wiederum wegen der Voraussetzung $qp^{\lambda-\varepsilon}$, ein Vielfaches von qp^λ sein und das ist nicht anders möglich, als wenn man ε gleich 0 annimmt, aber eben diese Annahme drückt den ausgesprochenen Satz aus.

Beispiele. Zu dem Exponenten 3 gehören nach dem Modul 9 die Zahlen 4 und 7 und in der That sind die Congruenzen

$$4^3 = 64 \equiv 1,\ 7^3 = 343 \equiv 1 \ ((mod\ 3^2))$$

leicht zu verificiren.

Wenn der Exponent, zu welchem x gehört, ein Theiler von $p-1$, aber eine relative Primzahl zu p ist, so wird der Satz gewöhnlich auch gelten, bis auf gewisse feststehende Ausnahmefälle von allgemeinerer Natur — aber, wenn auch nur äusserst sparsam gestreut, es kommen doch Fälle vor, in denen er seine Gültigkeit verliert.

So zum Beispiel gehört zu dem Exponenten 3 nach dem Modul 49 die Zahl 18 und zu dem Exponenten 5 nach dem Modul 11 die Zahlen 3 und 9 und gleichwohl bestehen im Widerspruche zu unserem Satze die Congruenzen

$$18^3 \equiv 1 \ ((mod\ 7^3)),$$

$$\left.\begin{array}{l} 3^5 \equiv 1 \\ 9^5 \equiv 1 \end{array}\right\} ((mod\ 11^2)),$$

welche alle 3 leicht zu verificiren sind. Bei dieser Gelegenheit ergiebt sich zugleich, dass 18 auch nach dem Modul $7^3 = 343$ zu dem Exponenten 3, sowie dass 3 und 9 auch nach dem Modul $11^2 = 121$ zu dem Exponenten 5 gehören.

Man hat endlich

$$14^{28} \equiv 1 \ ((mod\ 29^2 = 841))$$

und trotzdem gehört die Zahl 14 zu dem Exponenten 28 nicht allein etwa nach dem Modul 841, sondern auch nach dem Modul 29. Um nachzuweisen, dass 841 die höchste Potenz von 29 ist, welche die Differenz

$$14^{28}-1$$

theilt, bemerken wir, dass

$$14^7 = 105413505 = 125343 \,.\, 841 + 41$$

und mithin

$$14^{14} = 125343^2 \,.\, 841^2 + 82 \,.\, 125343 \,.\, 841 + 2 \,.\, 841 - 1$$

oder

$$14^{14} + 1 = 125343^2 \,.\, 841^2 + 1027828 \,.\, 841.$$

Da nun 29 in 1027828 nicht aufgeht, sondern den Rest 6 lässt, so ist 841 die höchste Potenz von 29, welche die Summe

$$14^{14}+1$$

theilt, und zugleich erhellt, dass die Differenz

$$14^{14}-1$$

überhaupt durch keine Potenz von 29 theilbar ist. Daraus folgt die Congruenz:

$$(14^{14}+1)(14^{14}-1) = 14^{28}-1 \equiv 1 \ ((mod\ 29^2)).$$

Mit diesen wenigen Beispielen sind aber auch alle erschöpft, die sich für eine unterhalb der Grenze 1000 befindliche Potenz einer ungeraden Primzahl als Modul auftreiben lassen, so dass x zu einem Exponenten, der grösser als 2 und relative Primzahl zu p ist, nach diesem Modul p^n gehört und dennoch p^n nicht die höchste Potenz ist, welche die Differenz

$$x^q-1$$

theilt. Das letzte ist besonders bemerkenswerth als ein Beleg, wie die Zahl x eine primitive Wurzel von p darstellen kann, ohne dass sie es gleichzeitig für die höheren Potenzen von p zu sein brauche — in der Regel wird dies freilich eintreffen.

Der oben erwähnten Ausnahmefälle von allgemeinerer Natur sind zwei; der erste ist die Zahl 1, welche für jeden Modul zu dem Exponenten 1 gehört, und der zweite ist die Zahl

$$-1 \equiv p^n - 1 \ (mod\ p^n),$$

welche gleichfalls für jeden Modul zu dem Exponenten 2 gehört; denn es ist

$$(-1)^2 \equiv 1 \ (mod\ p^n)$$

und offenbar die zweite Potenz von -1 die niedrigste gleich 1.

Betrachten wir jetzt den Fall

$$p = 2,$$

in welchem immer

$$q = 1$$

gesetzt werden muss, so ist der Ausnahmefall $\lambda = 0$ ohne alle wesentliche Bedeutung. Dagegen, und man sieht den Grund bei einer genauen Durchsicht des Beweises, der sich auf die Sätze *b*) und mittelbar *a*) stützt, ohne Mühe ein, muss n die Zahl 2 übersteigen und der Satz spricht sich daher, wie folgt, aus:

Wenn n eine Zahl grösser als 2 bezeichnet und die Zahl x gehört zu dem Exponenten 2^λ nach dem Modul 2^n, so ist immer

$$x^{2^\lambda} \equiv 1 \ ((mod\ 2^n)).$$

Nimmt man $n = 2$, so gehört die Zahl 3 in der That zu dem Exponenten 2 ebensowohl nach dem Modul 4, wie nach dem Modul 8: aber nur im letzteren Falle ist

$$3^2 \equiv 1 \ ((mod\ 2^3)).$$

Ebenso hat man

$$5^2 \equiv 1 \ ((mod\ 2^3)),$$
$$7^2 \equiv 1 \ ((mod\ 2^4)),$$

wo die Zahlen 5 und 7 zu dem Exponenten 2 gehören respective nach dem Modul 8 oder 16.

Der Vollständigkeit halber müssen wir noch erörtern, was eintritt, wenn x zu q gehört, ohne dass p^n die höchste Potenz sei, welche die Differenz

$$x^q - 1$$

theilt. Sei dieser höchste Theiler $p^{n+\omega}$, so ist

$$x^q \equiv 1 \ ((mod\ p^{n+\omega}))$$

und es lässt sich nachweisen, dass x zu q gehört nach der Reihe der Modul:

$$p^n\ p^{n+1},\ p^{n+2} \ldots\ldots p^{n+\omega}.$$

Bezeichnen wir zu dem Zwecke den Divisor von q, zu dem x nach irgend einem derselben, etwa $p^{n+\nu}$, gehört, vorläufig mit $\varkappa$, so hat man

$$x^\varkappa \equiv 1 \ (mod\ p^{n+\nu})$$

und hieraus

$$x^\varkappa \equiv 1 \ (mod\ p^n).$$

Mithin muss, zu Folge der Voraussetzung, $\varkappa$ ein Multiplum von q sein; nach der Annahme ist es aber zugleich ein Divisor von q. Dies beides ist nur so möglich, dass man $\varkappa = q$ annimmt.



d) Umkehrung des vorigen Satzes.

W e n n d i e $\varkappa$te P o t e n z v o n q d i e h ö c h s t e i s t , w e l c h e d i e D i f f e r e n z

$$x^{qp^\lambda}-1$$

t h e i l t , s o g e h ö r t d i e Z a h l x z u d e m E x p o n e n t e n qp^λ n a c h d e m M o d u l p^n.

Wir setzen den Exponenten, zu welchem x gehört, gleich $\varkappa p^\omega$, so darf man

$$\varkappa\varkappa' = q, \ \omega \overline{\overline{<}} \lambda$$

annehmen, weil der Exponent qp^λ offenbar ein Multiplum des letztgenannten sein muss. Indem dann gemäss dem vorigen Satze die Congruenz

$$x^{\varkappa p^\omega} \equiv 1 \ ((mod\ p^n))$$

bestehen muss, kann man nach *a*) weiter schliessen auf die Congruenz

$$x^{\varkappa p^\lambda} \equiv 1 \ ((mod\ p^{n+\lambda-\omega}))$$

und hieraus folgt durch Erhebung auf die $\varkappa'$te Potenz und Einsetzung des Werthes q für $\varkappa\varkappa'$

$$x^{qp^\lambda} \equiv 1 \ (mod\ p^{n+\lambda-\omega}).$$

Damit diese Congruenz nicht im Widerspruche zu der Voraussetzung stehe, muss man

$$n = n+\lambda-\omega, \text{ d. h. } \lambda=\omega$$

annehmen und unser Satz ist bewiesen.

Der Beweis passt nicht auf den Fall $\lambda=0$. Um ihn auch auf diesen auszudehnen bemerke man, d a s s , w e n n i r g e n d e i n E x p o n e n t $\varkappa$ d e r C o n g r u e n z

$$x^\varkappa \equiv 1 \ (mod\ p^n)$$

g e n ü g t , n o t h w e n d i g d i e C o n g r u e n z

$$x^{\varkappa p} \equiv 1 \ (mod\ p^{n+1})$$

b e s t e h e n m u s s. Denn aus der ersten folgt

$$x^\varkappa = 1+Xp^n,$$

also

$$x^{\varkappa p}-1 = p_1 Xp^n + p_2 X^2 p^{2n} + \ldots\ldots + X^p p^{pn}$$

und da die rechte Seite dieser Gleichung durch p^{n+1} getheilt werden kann, so muss dasselbe auch mit der linken Seite statt haben.

Sei also

$$x^q \equiv 1 \ ((mod\ p^n)),$$

so folgt nach *a*)

$$x^{qp} \equiv 1 \ ((mod\ p^{n+1}))$$

und mithin muss nach *c*) x zu dem Exponenten qp gehören nach dem Modul p^{n+1}. Wir wollen nun darthun, dass x nach dem Modul p^n zu q gehört. Wenn es nicht zu q gehört, so muss es zu irgend einem Factor $\varkappa$ von q gehören, also:

$$x^{\varkappa} \equiv 1 \ (mod\ p^n).$$

Hieraus schliesst man zu Folge der eben gemachten Bemerkung:

$$x^{\varkappa p} \equiv 1 \ (mod\ p^{n+1})$$

und es müsste demgemäss $\varkappa p$ ein Multiplum von qp sein, was nicht angeht, da $\varkappa$ ein Factor von q sein soll, es sei denn, dass man $\varkappa = q$ habe.

3) Die erörterten Principien enthalten die Fundamente einer Theorie, vermöge derer man in den Stand gesetzt wird, die zu den Theilern von

$$\pi = (p-1)p^n$$

gehörigen Zahlen zu bestimmen vermöge derjenigen Zahlen, welche zu den Theilern von $p-1$ nach dem Modul p gehören. Indessen ist es kürzer sich zuerst eine primitive Wurzel von p^n zu berechnen und auf deren Betrachtung dann alles Uebrige zurückzuführen, wie es nach Analogie des Falles $n=1$ möglich sein muss. Dies Geschäft wird ungemein vereinfacht, nämlich auf die Bestimmung einer primitiven Wurzel von p^2 zurückgebracht, durch das folgende Theorem:

Jede primitive Wurzel des Moduls p^2 ist auch eine primitive Wurzel des Moduls p^n und umgekehrt, jede primitive Wurzel des Moduls p^n ist eine primitive Wurzel des Moduls p^2 (die Zahl p als ungerade vorausgesetzt).

Der Beweis ist äusserst einfach. Wenn wir unter g eine primitive Wurzel von p^2 verstehen, so ist der zugehörige Exponent

$$\pi = (p-1)p$$

und es besteht nach *c*) die Congruenz

$$g^{(p-1)p} \equiv 1 \ ((mod\ p^2)).$$

Mithin folgt nach *a*)

$$g^{(p-1)p^{n-1}} \equiv 1 \ ((mod\ p^n))$$

und es muss daher nach *d*) g nach dem Modul p^n zu dem Exponenten $(p-1)p^{n-1}$ gehören, d. h. eine primitive Wurzel von p^n sein.

Der Beweis für die Umkehrung ist eben so leicht. Aus der Congruenz

$$g^{(p-1)p^{n-1}} \equiv 1 \ ((mod\ p^n))$$

folgt vermöge des Satzes *b* unter voriger Nummer

$$g^{(p-1)p} \equiv 1 \ ((mod\ p^2))$$

und hieraus, wieder durch Anwendung von *d*), dass g eine primitive Wurzel von p^2 ist.

Es ist jetzt zu zeigen, wie man unter allen Umständen mindestens eine primitive Wurzel des Moduls p^2 finden kann.

Sei irgend eine der zu p gehörigen primitiven Wurzeln g; dann wird in der Regel die Differenz

$$g^{p-1}-1$$

nicht durch p^2 theilbar sein; es ist mithin

$$g^{p-1} \equiv 1 \ ((mod\ p)),$$

daraus folgt aber nach dem Satze *a*) der vorigen Nummer, dass

$$g^{(p-1)p} \equiv 1 \ ((mod\ p^2))$$

und mithin muss g auch eine primitive Wurzel von p^2 sein, gemäss dem Theoreme *d*).

Sollte aber, was nur selten eintritt, die erwähnte Differenz durch p^2 theilbar sein, so setze man

$$g' = g + hp,$$

wo h irgend eine durch p nicht theilbare Zahl bezeichnet und bilde die Potenzgleichung

$$g'^{p-1}-1 = g^{p-1}-1+(p-1)_1 g^{p-2}hp+(p-1)_2 g^{p-3}h^2p^2$$
$$+\dots\dots+(p-1)_{p-1}h^{p-1}p^{p-1},$$

so erhellt durch Betrachtung der rechten Seite, dass die linke Seite einmal durch p theilbar ist und dann, dass sie durch keine höhere Potenz von p als die erste getheilt werden kann. Das Erste ist unmittelbar klar, da $g^{p-1}-1$ nach der Voraussetzung sogar durch p^2 theilbar ist, alle anderen Glieder der Reihe aber p als Factor enthalten. Das zweite findet statt, weil alle Glieder der Reihe ersichtlich p^2 oder noch höhere Potenzen von p als Theiler haben mit einziger Ausnahme des zweiten Gliedes

$$(p-1)_1 g^{p-2}hp,$$

welches, da g und h relative Primzahlen zu p sind, nur durch die erste Potenz von p aufgeht. Mithin bleibt wegen desselben bei der Division mit p^2 ein Rest.

Da hiernach die Congruenz

$$g'^{p-1} \equiv 1 \ ((mod\ p))$$

besteht, so folgt nach dem Satze *a)* der vorigen Nummer

$$g'^{(p-1)p} \equiv 1 \ ((mod\ p^2))$$

und es muss nach *d)* die Zahl

$$g' = g + hp$$

eine primitive Wurzel des Moduls p^2 sein.

Fassen wir die Resultate unserer Entwickelung zusammen, so haben wir das folgende Theorem:

Wenn g irgend eine primitive Wurzel von p ist, so ist es im Allgemeinen auch eine primitive Wurzel von p^2, nämlich wenn man gleichzeitig

$$g^{p-1} \equiv 1 \ ((mod\ p))$$

hat; wird dagegen diese Congruenz in dem angedeuteten Nebensinne nicht befriedigt, so ist, wenn h irgend eine der Zahlen

$$1 \ 2 \ 3 \ 4 \ldots\ldots\ldots\ldots p-1$$

bezeichnet, die primitive Wurzel von p^2 irgend eine Zahl von der Form

$$g' = g + hp.$$

Beispiel 1. Es sei

$$p = 13,\ p^2 = 169.$$

Die primitiven Wurzeln von 13 sind bekanntlich

$$2 \ 6 \ 7 \ 11$$

und man hat:

$$2^{12} - 1 = (2^6 - 1)\ (2^6 + 1) = 63.65.$$
$$6^{12} - 1 = (6^6 - 1)\ (6^6 + 1) = 46655.13.3589,$$
$$7^{12} - 1 = (7^6 - 1)\ (7^6 + 1) = 117648.13.9050$$
$$11^{12} - 1 = (11^6 - 1)(11^6 + 1) = 1771560.13.136274;$$

mithin geht in keine der genannten Differenzen 13^2 auf und es sind daher die untersuchten Zahlen sämmtlich primitive Wurzeln von 169.

Beispiel 2. Eine primitive Wurzel von 29 ist ± 14 und es ist, wie wir früher erkannt haben,

$$14^{28} \equiv 1 \ ((mod\ 29^2));$$

mithin gehört ± 14 nach dem Modul

$$p^2 = 841$$

zu dem Exponenten 28 und ist keine primitive Wurzel von 841. Um eine solche zu finden, setze man

$$g' = \pm 14 + 29h$$

und gebe dem h nach und nach alle Werthe von 1 bis $p-1=28$. Dadurch findet man folgende beiden Reihen primitiver Wurzeln:

43 72 101 826,
15 44 73 .... 798.

Um z. B. den Nachweis zu führen, dass 15 eine primitive Wurzel von 842 ist, bemerke man, dass nach dem Canon arithmeticus

$$15 \equiv 2^{27} \ (mod\ 841)$$

und mithin die Potenz

$$15^{\frac{\pi}{2}} = 15^{406} \equiv 2^{27 \cdot 406} \equiv 2^{10962}$$

ist. Sondert man hier die Vielfachen von

$$\pi = 812$$

ab, so bleibt

$$15^{\frac{\pi}{2}} \equiv 2^{406}$$

und dies ist, wie aus der angezeigten Tabelle folgt,

$$\equiv -1 \ (mod\ 841).$$

Wenn nun eine kleinere Zahl x als π zu 15 gehört, so ist klar, dass eine der Potenzen

$$1 \ 15^1 \ 15^2 \ 15^3 \ ..... \ 15^{x-1}$$

nothwendig den Rest -1 lassen muss, denn die Fortsetzung der Reihe giebt keine neuen Reste und einmal, wie wir gesehen haben, kommt man auf eine solche Potenz, nämlich

$$15^{\frac{\pi}{2}} \equiv -1 \ (mod\ 841).$$

Offenbar kann diese Potenz keine andere sein als $15^{\frac{x}{2}}$ und es ist daher

$$15^{\frac{x}{2}} \equiv -1 \ (mod\ 841).$$

Da nun x ein Divisor von π sein muss, so folgt, wenn die beiden letztgenannten Congruenzen einander nicht widerstreiten sollen, dass der Quotient

$$x' = \frac{\pi}{x}$$

ungerade ist; denn wäre er gerade, so gäbe die letzte Congruenz durch Erhebung auf die x'te Potenz

$$15^{\frac{\pi}{2}} \equiv +1 \ (mod\ 841).$$

Also wird umgekehrt x unter den Quotienten sich befinden, welche entstehen, wenn man π durch alle möglichen ungeraden Divisoren, die es hat, dividirt. Deren sind nun nicht mehr als folgende vier:

$$7.29 = 203,\ 29,\ 7,\ 1,$$

und ihnen entsprechen die Quotienten:

$$4\ \ 28\ \ 116\ \ 812.$$

Der letzte giebt offenbar 1 nach dem verallgemeinerten Lehrsatze von Fermat, die drei andern geben zu Folge der Tabelle bezüglich

$$15^4 \equiv 2^{4 \cdot 27} = 2^{108} \equiv 165,$$
$$15^{28} \equiv 2^{28 \cdot 27} = 2^{756} \equiv 784,$$
$$15^{116} \equiv 2^{116 \cdot 27} = 2^{3 \cdot 812 + 696} = 2^{696} \equiv 571.$$

Andere Exponenten, welche eine Potenz von 15 gleich 1 machen könnten und zugleich kleiner als π wären, existiren nicht, also ist 15 eine primitive Wurzel von 841.

Auf die beschriebene Art ist man immer in den Stand gesetzt wenigstens eine primitive Wurzel von p^2 und dem zu Folge auch von p^n mit leichter Mühe zu erhalten. Ist aber eine solche, die wir, wie gewöhnlich mit g bezeichnen, bekannt und man bildet sich die auf die Reihe der Potenzen

$$1\ g\ g^2\ g^3 \ldots\ldots g^{\pi-1}$$

bezügliche Restperiode, so kommen, in vollkommener Analogie mit dem Falle, wo der Modul die erste Potenz von p war, die sämmtlichen zu einem Exponenten

$$Q = qp^{\lambda}$$

gehörigen Zahlen mit den Resten aller solchen Potenzen von g überein, deren Exponenten kleiner als die Anzahl π und mit ihr zum grössten gemeinschaftlichen Theiler die Zahl

$$Q' = \frac{\pi}{Q} = \frac{p-1}{q} p^{n-\lambda-1}$$

haben. Es gehören mithin soviele Zahlen x zu dem Exponenten Q, als relative Primzahlen, die kleiner als er sind, existiren.

Sei m irgend eine relative Primzahl zu Q und kleiner als Q, so ist mQ' der entsprechende Exponent, der mit π den grössten gemeinschaftlichen Theiler Q' besitzt und wir sollen darthun, dass der Rest der Potenz

$$g^{mQ'} = g^{m\frac{p-1}{q}p^{n-\lambda-1}}$$

zu dem Exponenten Q gehört. In der That ist zunächst

$$(g^{mQ'})^Q = g^{mQQ'} = g^{m\pi} \equiv 1 \pmod{p^n}$$

und es muss nur noch gezeigt werden, dass keine niedrigere Potenz von $g^{mQ'}$ der Einheit gleich wird. Wäre x der zu $g^{mQ'}$ gehörige Exponent, so folgte

$$(g^{mQ'})^x = g^{mxQ'} \equiv 1 \pmod{p^n}$$

und es ergäbe sich, da g zu π gehört, dass mxQ' ein Vielfaches von $\pi = QQ'$ sein müsste. Dies setzte voraus, dass mx durch Q theilbar wäre, welches, da x ein Factor von Q und m relative Primzahl zu Q ist nicht anders möglich ist, als indem man $x = Q$ annimmt. Also gehört die Potenz $g^{mQ'}$ zu dem Exponenten Q.

Um den zweiten Theil unseres Satzes zu beweisen, bemerke man zunächst, dass alle solche Potenzen $g^{mQ'}$ von einander verschieden ausfallen — denn sie sind unter den $(\pi-1)$ ersten Potenzen von g enthalten, welche einander alle incongruent sind — und dann, dass jede Zahl, welche zu Q gehört, nothwendig eine Potenz von der Form $g^{mQ'}$ sein muss. Denn könnte z. B. g^{μ} zu Q gehören und dennoch Q' nicht der grösste gemeinschaftliche Theiler zwischen μ und π sein, so wäre μ kein Multiplum von Q'. Dieses muss es aber nothwendig sein, denn wenn die Congruenz

$$(g^{\mu})^Q = g^{\mu Q} \equiv 1 \pmod{p^n}$$

besteht, so folgt, dass μQ ein Vielfaches von

$$\pi = QQ'$$

ist, und dieses setzt μ als ein Vielfaches von Q' voraus. Also können nur soviele und nicht mehr zu Q gehörige Zahlen existiren, als es Zahlen $m < Q$ und relative Primzahlen zu Q giebt.

Um ein geeignetes Uebungsmaterial zu bieten, mögen die Resultate für die ersten Potenzen der Zahl 3, sowie für die zweite Potenz von 5 und 7 folgen:

q	$p^2=9$	
1	1	
2	—1	
3	4	—2
6	2	—4

q	$p^3=27$					
1	1					
2	—1					
3	10	—8				
6	8	—10				
9	4	7	13	—11	—5	—2
18	2	5	11	—13	—7	—4

q	$p^2=3^4=81$								
1	1								
2	—1								
3	28	—26							
6	26	—28							
9	10	19	37	—35	—17	—8			
18	8	17	35	—37	—19	—10			
27	4	7	13	16	22	25	31	34	40
	—38	—32	—29	—23	—20	—14	—11	—5	—2
54	2	5	11	14	20	23	29	32	38
	—40	—34	—31	—25	—22	—16	—13	—7	—4

q	$p^2=25$							
1	1							
2	—1							
4	7	—7						
5	6	11	—9	—4				
10	4	9	—11	—6				
20	2	3	8	12	—12	—8	—3	—2

q	$p^2=49$											
1	1											
2	—1											
3	18	—19										
6	19	—18										
7	8	15	22	—20	—13	—6						
14	6	13	20	—22	—15	—8						
21	2	4	9	11	16	23	—24	—17	—12	—10	—5	—3
42	3	5	10	12	17	24	—23	—16	—11	—9	—4	—2

Die gewonnenen Resultate können noch auf den Fall übertragen werden, wo der Modul die doppelte Potenz irgend einer ungeraden Primzahl wird, also

$$P = 2p^n.$$

Man erhält für diese Annahme

$$\pi = S'''P = (p-1)p^{n-1},$$

also dieselben Exponenten zu betrachten, wie wenn der Modul nur p enthielte.

Die Uebertragung vermittelt sich vermöge des Theoremes:

Jede ungerade Zahl, die zu dem Exponenten

$$Q = qp^\lambda$$

nach dem Modul p^n gehört, gehört zu dem nämlichen Exponenten auch nach dem Modul $2p^n$, und die Summe einer geraden Zahl, die zu dem Exponenten

$$Q = qp^\lambda$$

nach dem Modul p^n gehört, mit diesem Modul $\pm p^n$ liefert eine Zahl, die zu dem nämlichen Exponenten nach dem Modul $2p^n$ gehört.

Sei zunächst x eine ungerade Zahl, so ist

$$x^Q \equiv 1 \ (mod\ p^n)$$

und gleichzeitig

$$x^Q \equiv 1 \ (mod\ 2),$$

mithin, da die Modul 2 und p^n relative Primzahlen zu einander sind, zu Folge des 5ten Satzes in §. 4

$$x^Q \equiv 1 \ (mod\ 2p^n).$$

Wenn also x^Q erweislich die niedrigste Potenz von x ist, die zum Reste 1 lässt, so gehört x zu Q. Dies muss nun mit Nothwendigkeit statt haben; denn wäre die niedrigste Potenz die $\varkappa$te, so dass

$$x^\varkappa \equiv 1 \ (mod\ 2p^n),\ \varkappa < Q$$

wäre, so folgte

$$x^\varkappa \equiv 1 \ (mod\ p^n),$$

d. h. es gäbe eine niedrigere Potenz $x^\varkappa$ als die niedrigste x^Q, welche nach dem Modul p^n der Einheit gleich würde.

Sei ferner x eine gerade Zahl, so ist

$$x \pm p^n \equiv x \ (mod\ p^n)$$

und es gehört mithin auch $x \pm p^n$ zu dem Exponenten Q, mithin ist

$$(x \pm p^n)^Q \equiv 1 \ (mod\ p^n)$$

und gleichzeitig, weil $x \pm p^n$ eine ungerade Zahl ist,

$$(x \pm p^n)^Q \equiv 1 \ (mod\ 2);$$

aus diesen beiden Congruenzen ergiebt sich

$$(x \pm p^n)^Q \equiv 1 \ (mod\ 2p^n)$$

und es lässt sich nun ähnlich, wie vorher, darthun, dass $(x \pm p^n)^Q$ die niedrigste der Einheit congruente Potenz von $x \pm p^n$ ist. Also gehört $x \pm p^n$ zu dem Exponenten Q nach dem Modul $2p^n$.

Dieses vorausgesetzt lässt sich, mag nun P die Form p^n oder $2p^n$ haben, der nämliche Satz beweisen, der für die erste Potenz von p als Modul bereits bewiesen ist, nämlich:

Wenn x zu dem Exponenten Q nach dem Modul

$$P = p^n,\ 2p^n$$

gehört und man bildet sich die Zahlenreihe

$$1 \quad m' \quad m'' \quad m''' \ \ldots\ldots \ Q-1,$$

welche alle relativen Primzahlen zu Q unterhalb dieser Zahl enthält, so sind die sämmtlichen diesem Exponenten zugehörigen Zahlen den Potenzen

$$x \quad x^{m'} \quad x^{m''} \quad x^{m'''} \ \ldots\ldots \ x^{Q-1}$$

nach dem Modul P congruent.

Es besteht ferner in beiden Fällen das schöne Theorem, dass, wenn g eine primitive Wurzel des Moduls P bezeichnet, die Reste der Potenzen

$$1 \quad g \quad g^2 \quad g^3 \quad g^4 \ \ldots\ldots\ldots \ g^{\pi-1}$$

alle unter einander verschieden sind und mit den relativen Primzahlen zu P, die kleiner als P sind, übereinkommen.

Die Beweise können wir, da sie keine neuen Gesichtspuncte darbieten, füglich übergehen. Dagegen dürfte es nicht unzweckmässig sein, einige auf den Modul $2p^n$ bezügliche durchgeführte Beispiele folgen zu lassen:

q	$2p^2=18$	
1	1	
2	—1	
3	7	—5
6	5	—7

q	$2p^2=54$					
1	1					
2	—1					
3	19	—17				
6	17	—19				
9	7	13	25	—23	—11	—5
18	5	11	23	—25	—13	—7

q	$2p^2=50$							
1	1							
2	—1							
4	7	—7						
5	11	21	—19	—9				
10	9	19	—21	—11				
20	3	13	17	23	—23	—17	—13	—3

Schliesslich müssen wir noch den speciellen Fall

$$P=2^n$$

erörtern. Hier tritt nun der bemerkenswerthe Umstand ein, dass das Fermat'sche Theorem eine wesentliche Modification erfährt. Ehe wir dieselbe herleiten, schicken wir die Bemerkung voraus, dass wir von den beiden Fällen

$$P=2,\ 2^2$$

gänzlich absehen und mithin n immer grösser als 2 annehmen. Dadurch gewinnen wir den Vortheil, dass wir alle einleitenden Sätze der vorigen Nummer ohne Einschränkung anwenden können und also der speciellen Erwähnung bedeutungsloser Ausnahmefälle überhoben bleiben.

Indem wir unter x eine beliebige ungerade Zahl verstehen, muss es nothwendig entweder von der Form

$$4h+1$$

oder von der Form

$$4h-1$$

sein; wir erhalten demgemäss

$$x^2=16h^2\pm 8h+1$$

und erkennen, dass das Quadrat jeder ungeraden Zahl mindestens durch 2^3 theilbar sei. Daher ist allgemein

$$x^2\equiv 1 \ (mod\ 2^3).$$

Nun folgt nach der Schlussbemerkung, die wir in der vorigen Nummer gemacht haben, dass, wenn

$$x^{\varkappa} \equiv 1 \ (mod\ p^n),$$

hieraus nothwendig

$$x^{\varkappa p} \equiv 1 \ (mod\ p^{n+1})$$

folge. Indem wir diesen Satz auf die soeben erhaltene Congruenz anwenden, folgt allmählig

$$x^{2^2} \equiv 1 \ (mod\ 2^4),$$
$$x^{2^3} \equiv 1 \ (mod\ 2^5),$$

. . . . .

. . . . .

$$x^{2^{n-2}} \equiv 1 \ (mod\ 2^n)$$

und das Theorem von Fermat heisst daher für $P = 2^n$, wie folgt:

Wenn der Modul irgend eine beliebige die zweite übersteigende Potenz von 2 und x eine beliebige ungerade Zahl ist, so besteht immer die Congruenz:

$$x^{2^{n-2}} \equiv 1 \ (mod\ 2^n).$$

Wir werden daher jetzt, der Analogie halber, wenn keine niedrigere Potenz von x der Einheit gleich wird, dieselbe eine primitive Wurzel von 2^n nennen, und können auch, wie man sich ohne Mühe überzeugt, alle solche Exponenten, zu denen irgend welche x gehören, als Divisoren von 2^{n-2} ansehen.

Betrachten wir x unter einer der beiden Formen:

$$4h+1, \ 4h-1,$$

so dass wir darin h als eine ungerade Zahl voraussetzen, so ist offenbar

$$x^2 \equiv 1 \ ((mod\ 2^3));$$

mithin nach dem Satze a) der vorigen Nummer

$$x^{2^{n-3}} \equiv 1 \ ((mod\ 2^n)),$$

also, zu Folge des Satzes d) in derselben Nummer, gehört x zu dem Exponenten 2^{n-2}. Bedenken wir jetzt, dass, wenn man in $4h \pm 1$ für h die allgemeine Zahlform $2k+1$ einsetzt, unter der alle ungeraden Zahlen stehen, man respective

$$8k+5 = 8k+8-3, \ 8k-3$$

erhält, so kann man jetzt das Theorem aussprechen:

Alle Zahlen von der Form $8k \pm 3$ sind primitive Wurzeln von 2^n.

Indem man die noch übrigen bleibenden Zahlen, die nothwendig eine der beiden Formen

$$8k+1,\ 8k-1$$

haben müssen, betrachtet, kommt man durch Induction leicht auf folgendes allgemeinere Theorem: Alle Zahlen der Form

$$2^\lambda h \pm 1$$

gehören, unter der Voraussetzung, dass h nur ungerade Zahlenwerthe anzeigt, nach dem Modul 2^n zu dem Exponenten $2^{n-\lambda}$.

Es ist nämlich, wenn man

$$x^2 = (2^\lambda h \pm 1)^2 = 2^{2\lambda} h^2 + 2^{\lambda+1} h + 1$$

setzt, unter der Voraussetzung ungerader Zahlenwerthe h ersichtlich

$$x^2 \equiv 1 \ ((mod\ 2^{\lambda+1})),$$

mithin folgt nach a)

$$x^{2^{1+n-\lambda-1}} \equiv 1 \ ((mod\ 2^{\lambda+1+n-\lambda-1}))$$

oder einfacher

$$x^{2^{n-\lambda}} \equiv 1 \ ((mod\ 2^n)),$$

und es muss also x zu dem Exponenten $2^{n-\lambda}$ gehören.

Wenn g eine beliebige primitive Wurzel von 2^n ist und man bildet sich die Reihe der Potenzen

$$1 \quad g \quad g^2 \quad g^3 \ \ldots\ldots \ g^{2n-1},$$

so weiss man, dass die Reste alle verschieden ausfallen; aber sie kommen nicht mehr, wie in den früheren Fällen, mit der Reihe der sämmtlichen Zahlen überein, welche relative Primzahlen zu 2^n und kleiner als 2^n sind: dazu reicht ihre Anzahl nicht aus, denn dieselbe ist

$$2^{n-2} = \frac{1}{2} S'''2^n.$$

Man kann aber die Zahlform, unter der diese Reste stehen, zum Voraus bestimmen. Die primitive Wurzel g nämlich ist nothwendig von der Form

$$g = 8h \pm 3;$$

hieraus folgt:

$$g^{2n} = (8h)^{2n} \pm (2n)_1 (8h)^{2n-1}.3 + \ldots\ldots \pm (2n)_1 8h.3^{2n-1} + 3^{2n},$$
$$g^{2n+1} = (8h)^{2n+1} \pm (2n+1)_1 (8h)^{2n}.3 + \ldots\ldots + (2n+1)_1 8h.3^{2n} \pm 3^{2n+1}$$

oder da alle geraden Potenzen von 3 durch 8 getheilt die Zahl 1 zum Rest lassen und folgeweise alle ungeraden Potenzen die Zahl 3 zum Reste haben:

$$g^{2n} = 8H+1,$$
$$g^{2n+1} = 8H\pm 3.$$

Demgemäss, wenn die primitive Wurzel g die Form $8h+3$ hat, so sind die Glieder der Restperiode die sämmtlichen ungeraden Zahlen, bis zur Grenze 2^n, welche von der Form

$$8H+1,\ 8H+3$$

sind; dagegen wenn die primitive Wurzel von der Form $8h-3$ ist, so sind die Glieder der Restperiode aller ungeraden Zahlen von der Form

$$8H+1,\ 8H-3;$$

die Form

$$8H-1$$

mithin kann unter den Resten keinesfalls vorkommen.

Beispiele:

q	8
1	1
2	—1 3 —3

q	16
1	1
2	—1 7 —7
4	3 5 —5 —3

q	32
1	1
2	—1 15 —15
3	7 9 —9 —7
	3 5 11 13 —13 —11 —5 —3

q	64
1	1
2	—1 31 —31
4	15 17 —17 —15
8	7 9 23 25 —25 —23 —9 —7
16	3 5 11 13 19 21 27 29 —29 —27 —21 —19 —13 —11 —5 —3

4) Was nun die Auflösung der allgemeinen Congruenz

$$x^N \equiv r\ (mod\ P = p^n,\ 2p^n),$$

wo r natürlich eine relative Primzahl zu P bezeichnet, anbetrifft, so gelten hier, bis auf das Detail der Beweise selbst, genau die nämlichen Principien, wie in dem besonderen Falle, den wir im vorhergehenden Paragraphen weitläufig erörtert haben. Wir begnügen uns daher um so mehr mit einer Recapitulation, da einzelne Puncte demungeachtet auch in den nachfolgenden Entwickelungen ihre Begründung finden.

Wenn N eine relative Primzahl zu π ist, so hat die Congruenz eine reelle Wurzel und sonst keine anderen, nämlich

$$x \equiv r^z \pmod{P},$$

wo z, indem q den zu r nach dem Modul gehörigen Exponenten bezeichnet, durch die Congruenz

$$Nz \equiv 1 \pmod{q}$$

sich bestimmt.

Wenn dagegen N und π keine relativen Primzahlen zu einander sind, sondern die Zahl Q zum grössten gemeinschaftlichen Theiler haben, so existiren, wenn die Congruenz anders möglich ist, Q von einander verschiedene Lösungen und sonst keine anderen. Die Möglichkeit der Congruenz hängt davon ab, ob a ein Rest oder Nichtrest der Qten Potenz sein kann; sie ist demgemäss möglich, wenn die Bedingungscongruenz

$$r^{\frac{\pi}{Q}} = r^{Q'} \equiv 1 \pmod{P}$$

erfüllt wird und unmöglich, wenn dieselbe nicht erfüllt wird.

Ihre Möglichkeit vorausgesetzt lässt sich die vorgelegte Congruenz immer auf eine solche Congruenz

$$y^Q \equiv r \pmod{P}$$

zurückführen, in welcher Q ein Factor von π ist; denn die Q Lösungen der letzteren nach y liefern uns die Q Congruenzen

$$x^{N'} = x^{\frac{N}{Q}} \equiv y \pmod{P},$$

deren Auflösung nach x die sämmtlichen möglichen Wurzeln unserer vorgegebenen Congruenz giebt.

Betrachten wir mithin jetzt die specielle Congruenz

$$x^Q \equiv r \pmod{P};$$

auf welche wir in jedem einzelnen Falle schliesslich zurückkommen, so beruht ihre Lösung auf dem Theoreme, dass, wenn man sich die Reihe der Potenzen

$$1 \quad m'^Q \quad m''^Q \quad m'''^Q \quad \ldots\ldots \quad (P-1)^Q$$

bildet (wo die Zahlen

$$1 \quad m' \quad m'' \quad \ldots\ldots \quad P-1,$$

wie gewöhnlich alle unterhalb der Grenze P liegenden relativen Primzahlen zu P bezeichnen), sich deren Reste in Q' Gruppen zu je Q Zahlen vertheilen, so dass die Reste r einer jeden Gruppe

gleich, die ihnen entsprechenden Zahlen m dagegen verschieden sind.

Die Art der Verknüpfung, welche zwischen den Zahlen und den bezüglichen Resten eintritt, wird durch das Zusammenbestehen der beiden Congruenzen

$$\left.\begin{array}{l} x^{Q} \equiv r \\ r^{Q'} \equiv 1 \end{array}\right\} (mod\ P)$$

ausgesprochen. In der That geben die Q' von einander verschiedenen Lösungen der letzteren nach r die Q' von einander verschiedenen Congruenzen

$$x^{Q} \equiv r'\ r''\ r''' \ldots\ldots r^{(Q')}\ (mod\ P)$$

und diese nach x aufgelöst liefern $Q.Q'$ von einander verschiedene Zahlenwerthe von x, die offenbar mit der Reihe der relativen Primzahlen zu P bis zu dieser Grenze hin zusammenfallen.

Da die beiden eben erwähnten Congruenzen wohl nothwendig zusammen bestehen, aber nicht die eine aus der andern ihre Ableitung findet, so liegt hierin die Unmöglichkeit, dass die Auflösung der einen ein reeller Gewinn für die Auflösung der anderen ist. Also kann die Auflösung der Congruenz

$$x^{Q} \equiv r\ (mod\ P)$$

nicht mit strenger Nothwendigkeit auf den speciellen Fall $r = 1$ zurückgeführt werden und die Berechnung der diesem Falle entsprechenden Tabellen reicht noch nicht für die Lösung der allgemeinen Aufgabe aus.

Um aller Versuche überhoben zu sein (immer vorausgesetzt, dass der Canon arithmeticus nicht zur Verfügung steht), müssen hiernach noch Tabellen hinzutreten, die sich auf die verschiedenen Q' möglichen Werthe der Grösse r beziehen und aus denen man in jedem einzelnen Falle die dem betrachteten r entsprechenden Werthe von x entnehmen kann.

Diese Tabellen gestatten eine doppelte Abkürzung, einmal nach der Seite der x hin, die sie enthalten müssen und dann nach der Seite der Theiler von

$$\pi = S^{m}P,$$

auf welche sie sich zu beziehen haben.

Rücksichtlich der x brauchen nicht alle Werthe der Grösse x, die sich auf ein specielles x beziehen, aufgeführt zu werden, sondern es ge-

nügt ein einziger Werth. Ist nämlich ein solcher Werth R, so ist

$$x \equiv R \pmod P$$

eine Wurzel der Congruenz

$$x^Q \equiv r \pmod P$$

und, wenn h eine zu Q nach dem Modul P gehörige Zahl bezeichnet, so werden die sämmtlichen Wurzeln dargestellt durch die Reihe der Congruenzen

$$x \equiv R \; Rh \; Rh^2 \; \ldots\ldots \; Rh^{Q-1} \pmod P.$$

Rücksichtlich der Q brauchen nur solche Theiler von π berücksichtigt zu werden, welche absolute Primzahlen sind.

Denn sei Q eine zusammengesetzte Zahl, etwa

$$Q = a^\alpha \; b^\beta \; c^\gamma \ldots.$$

so können die Reste, welche die Qte Potenz möglicher Weise lassen kann, immer aus den Resten berechnet werden, welche respective die $a$te, $b$te, $c$te .... Potenz lassen. Wir werden diese Behauptung beweisen, indem wir von den einfacheren Fällen zu den zusammengesetzten aufsteigen und dabei noch einige nützliche Bemerkungen, welche frühere Entwickelungen ergänzen, zu machen Gelegenheit finden.

a) Vermöge der Tabellen, welche am Schlusse des vorigen Paragraphen für die Reste einiger Potenzen nach dem Modul 61 aufgestellt sind, kommt man zu dem Schlusse, dass, wenn wir die Reste zweier Potenzen, von denen der Exponent der ersten ein Theiler ist von dem Exponenten der zweiten, mit einander vergleichen, die Reste der zweiten Potenz sich sämmtlich unter den Resten der ersten Potenz vorfinden.

So z. B. erhält man für die Exponenten 2, 4, 6, 8, 10, 12 folgende Restperioden:

$$x^n \equiv r \pmod{61}.$$

$n=2$	$r=$	± 1	± 3	± 4	± 5	± 9	± 12	± 13	± 14	± 15	± 16	± 19	± 20	± 22	± 25	± 27
$n=4$	$r=$	$+1$	-3	-4	-5	$+9$	$+12$	$+13$	-14	$+15$	$+16$	-19	$+20$	$+22$	$+25$	-27
$n=6$	$r=$	± 1	± 3			± 9							± 20			± 27
$n=8$	$r=$	$+1$	-3	-4	-5	$+9$	$+12$	$+13$	-14	$+15$	$+16$	-19	$+20$	$+22$	$+25$	-27
$n=10$	$r=$	± 1						± 13	± 14							
$n=12$	$r=$	$+1$	$+3$			$+9$							$+20$			$+27$

Seien die Exponenten der beiden betrachteten Potenzen respective a und am und die ihnen zugehörigen Reste respective r und ϱ, so sind die beiden Congruenzen

$$\left.\begin{array}{l} x^a \equiv r \\ x^{am} \equiv \varrho \end{array}\right\} (mod\ P)$$

immer möglich, welche speciellen Restzahlen unter r und ϱ auch verstanden werden mögen. Bemerken wir nun, dass die Potenz x^m nothwendig irgend einer der Zahlen von 1 bis $P-1$ congruent sein muss und sei diese Zahl ξ, so folgt die dritte Congruenz

$$x^m \equiv \xi\ (mod\ P),$$

welche auf die $a$te Potenz erhoben und dann mit der dritten verglichen uns

$$\xi^a \equiv \varrho\ (mod\ P)$$

liefert, d. h. der Rest ϱ ist auch ein Rest der $a$ten Potenz, wie zu beweisen war. Zugleich erhellt, dass dieser Satz unabhängig von der Natur des Moduls P gilt, weil wir im Beweise nirgends genöthigt waren, ihn unter einer der speciellen Formen p^n oder $2p^n$ zu denken.

b) **Wenn Q der grösste gemeinschaftliche Theiler zwischen den beiden Exponenten N und π ist, so hat die Nte Potenz dieselben Reste, wie die Qte.**

Z. B. für die 5, 35, 3 und 9te Potenz erhält man folgende Reste:

$$x^n \equiv r\ (mod\ 61).$$

n	r
$n = 5$ $n = 35$	$r = 1$ 11 13 14 21 29 -29 -21 -14 -13 -11 -1
$n = 3$ $n = 9$	$r = \pm 1$ ± 3 ± 8 ± 9 ± 11 ± 20 ± 23 ± 24 ± 27 ± 28

Der Satz folgt unmittelbar aus der vorangehenden Bemerkung, dass die Congruenz

$$x^N \equiv r\ (mod\ P)$$

nur dann möglich ist, wenn gleichzeitig die Bedingungscongruenz

$$r^{Q'} = r^{\frac{\pi}{Q}} \equiv 1\ (mod\ P)$$

besteht, d. h. jeder Rest r der Nten Potenz muss eine Wurzel dieser letzten Congruenz sein. Dieselbe Bedingungscongruenz ist aber auch er-

forderlich, damit die Congruenz

$$x^Q \equiv r \pmod P$$

Bestand habe; mithin bekommen wir dieselben Zahlen, die wir als Rest der Nten Potenz bekommen haben, auch als Rest der Qten Potenz.

Zugleich ist in dem Vorhergehenden die Methode angegeben, vermöge deren man von den Lösungen der zuletzt genannten Congruenz zu den Lösungen unserer Ausgangscongruenz gelangen kann, d. h. vermöge deren man von dem Zahlenwerthe für x, welche r als Rest der Qten Potenz geben, man zu denjenigen Zahlenwerthen von x kommt, welche eben dieses r als Rest der Nten Potenz geben.

c) Wenn a^α irgend einen beliebigen Theiler von π bezeichnet, so lässt sich die Congruenz

$$x^{a^\alpha} \equiv r \pmod P$$

vom (a^α)ten Grade auf α Congruenzen vom $a$ten Grade zurückführen.

Man setze der Reihe nach die Congruenzen vom $a$ten Grade

$$\left.\begin{aligned} r &\equiv R^{(\alpha-1)a} \\ R^{(\alpha-1)} &\equiv R^{(\alpha-2)a} \\ R^{(\alpha-2)} &\equiv R^{(\alpha-3)a} \\ &\cdots\cdots \\ &\cdots\cdots \\ &\cdots\cdots \\ R''' &\equiv R''^a \\ R'' &\equiv R'^a \\ R' &\equiv R^a \end{aligned}\right\} \pmod P$$

Dies giebt zusammen α verschiedene Congruenzen und wenn sie sämmtlich möglich sind, so folgt durch allmählige Substitution

$$\left.\begin{aligned} r &\equiv R^{(\alpha-1)a} \\ r &\equiv R^{(\alpha-2)a^2} \\ r &\equiv R^{(\alpha-3)a^3} \\ &\cdots\cdots \\ &\cdots\cdots \\ r &\equiv R''^{a^{\alpha-2}} \\ r &\equiv R'^{a^{\alpha-1}} \\ r &\equiv R^{a^\alpha} \end{aligned}\right\} \pmod P$$

und es springt in die Augen, dass

$$x \equiv R \pmod P$$

eine Lösung der vorgelegten Congruenz sein muss.

Diese Folgerung ist indessen nur dann zwingend, wenn die obigen Congruenzen alle möglich sind, d. h. wenn die α Bedindungscongruenzen

$$\begin{aligned} r^{\frac{\pi}{a}} &\equiv 1 \\ R^{(\alpha-1)\frac{\pi}{a}} &\equiv 1 \\ R^{(\alpha-2)\frac{\pi}{a}} &\equiv 1 \\ \cdots\cdots & \qquad \pmod P \\ \cdots\cdots & \\ R'''^{\frac{\pi}{a}} &\equiv 1 \\ R''^{\frac{\pi}{a}} &\equiv 1 \\ R'^{\frac{\pi}{a}} &\equiv 1 \end{aligned}$$

alle zugleich erfüllt werden. Dieselben sind zu Folge der ursprünglich gesetzten Congruenzen identisch mit den folgenden:

$$\begin{aligned} r^{\frac{\pi}{a}} &\equiv 1 \\ R^{(\alpha-1)^{a\frac{\pi}{a^2}}} &\equiv r^{\frac{\pi}{a^2}} \equiv 1 \\ R^{(\alpha-2)^{a^2\frac{\pi}{a^3}}} &\equiv r^{\frac{\pi}{a^3}} \equiv 1 \\ \cdots\cdots\cdots & \qquad \pmod P \\ \cdots\cdots\cdots & \\ R'''^{a^{\alpha-3}\frac{\pi}{a^{\alpha-2}}} &\equiv r^{\frac{\pi}{a^{\alpha-2}}} \equiv 1 \\ R''^{a^{\alpha-2}\frac{\pi}{a^{\alpha-1}}} &\equiv r^{\frac{\pi}{a^{\alpha-1}}} \equiv 1 \\ R'^{a^{\alpha-1}\frac{\pi}{a^{\alpha}}} &\equiv r^{\frac{\pi}{a^{\alpha}}} \equiv 1 \end{aligned}$$

und diesen geschieht sämmtlich Genüge, sobald die letzte erfüllt wird; denn aus dieser lassen sich alle vorhergehenden durch angemessene Potenzirungen ableiten. Nun geschieht der letzten wirklich Genüge; denn wir haben die Grösse r als einen Rest der a^{α}ten Potenz angenommen, also ist das Nämliche mit allen vorhergehenden der Fall, d. h. die obigen α Hülfscongruenzen sind ohne Ausnahme möglich.

Das System der α Hülfscongruenzen vom $a$ten Grade ist der Ausgangscongruenz vom a^{α}ten Grade vollkommen identisch; darum muss es sämmt-

liche a^{te} Wurzeln der letzteren liefern. In der That bekommen wir allmählig a Werthe für jede der Grössen

$$R^{(\alpha-1)}\quad R^{(\alpha-2)}\quad R^{(\alpha-3)}\quad \ldots\ldots\quad R''\quad R'\quad R,$$

und es erhellt, dass, wenn diese Werthe alle für die jedes Mal nachfolgenden Congruenzen in Anspruch genommen werden, sie schliesslich a^α Werthe der Grösse R zusammensetzen.

Beispiel. Man soll die Restperiode der 8ten Potenz bestimmen in Bezug auf den Modul 73.

Die quadratischen Reste vertheilen sich wie folgt:

$$x^2 \equiv r \pmod{73}$$

r	x		r	x		r	x		r	x	
1	1	—1	18	23	—23	—36	16	—16	—16	35	—35
2	32	—32	19	26	—26	—35	29	—29	—12	34	—34
3	21	—21	23	13	—13	—32	25	—25	— 9	8	— 8
4	2	— 2	24	30	—30	—27	22	—22	— 8	24	—24
6	15	—15	25	5	— 5	—25	11	—11	— 6	33	—33
8	9	— 9	27	10	—10	—24	7	— 7	— 4	19	—19
9	3	— 3	32	18	—18	—23	14	—14	— 3	17	—17
12	31	—31	35	20	—20	—19	28	—28	— 2	12	—12
16	4	— 4	36	6	— 6	—18	36	—36	— 1	27	—27

Um nun die sämmtlichen Zahlen zu erhalten, welche Reste der 8ten Potenz sein können, muss man die Bedingungscongruenz

$$r^{\frac{p-1}{a^\alpha}} \equiv r^9 \equiv 1 \pmod{73}$$

sich auflösen. Die kleinste der zu dem Exponenten 9 gehörigen Zahlen ist 2; mithin sind die sämmtlichen Lösungen der letzten Congruenz oder, was dasselbe ist, die Reste der 8ten Potenz den Potenzen

$$1\quad 2\quad 2^2\quad 2^3\quad 2^4\quad 2^5\quad 2^6\quad 2^7\quad 2^8$$

congruent; sie bilden also die Reihe der Zahlen

$$r = 1\quad 2\quad 4\quad 8\quad 16\quad 32\quad —9\quad —18\quad —36.$$

Um nun die Zahlenwerthe von x zu finden, welche einen speciellen Rest r geben, hat man nach einander die 3 Congruenzen

$$\begin{aligned} r &\equiv R''^2 \\ R'' &\equiv R'^2 \pmod{73} \\ R' &\equiv R^2 \end{aligned}$$

für die verschiedenen Zahlenwerthe von r aufzulösen. Man übersieht bald, ass die Auflösung sich jedes Mal geradezu aus der vorstehenden Tabelle

ablesen lässt und kann das Geschäft der Auflösung in folgender Uebersicht sich zusammenstellen:

r	1				2				4			
R''	1		—1		32		—32		2		—2	
R'	1	— 1	27	—27	18	—18	25	—25	32	—32	12	—12
$x \equiv R =$	+1	27	10	22	23	36	5	11	18	25	31	34
	— 1	—27	—10	—22	—23	—36	—5	—11	—18	—25	—31	—34

r	8				16				32			
R''	9		—9		4		—4		18		—18	
R'	3	—3	8	—8	2	—2	19	—19	23	—23	36	—36
$x \equiv R =$	21	17	9	24	32	12	26	28	13	14	6	16
	—21	—17	—9	—24	—32	—12	—26	—28	—13	—14	—6	—16

r	—9				—18				—36			
R''	8		—8		36		—36		16		—16	
R'	9	—9	24	—24	6	—6	16	—16	4	—4	35	—35
$x \equiv R =$	3	8	30	7	15	33	4	35	2	19	20	29
	—3	—8	—30	—7	—15	—33	—4	—35	—2	—19	—20	—29

d) Aus dem Satze *a*) ergiebt sich sogleich, dass, wenn ein Exponent sich irgendwie zusammensetzt, also

$$Q = a^\alpha \, b^\beta \, c^\gamma \, ... \, l^\lambda$$

die Reste der Qten Potenz nothwendig mit denjenigen Resten der auf die Exponenten

$$a^\alpha \quad b^\beta \quad c^\gamma \, ...$$

bezüglichen Potenzen zusammenfallen müssen, welche allen diesen verschiedenen Restreihen gemeinschaftlich sind. Als Beispiele wollen wir wieder einige auf den Modul 61 bezügliche Restperioden betrachten und zwar wählen wir die Potenzen x^2, x^3, x^4, x^5, x^6, x^{10}, x^{12}, x^{15}.

$$x^n \equiv r \ (mod\ 61).$$

$n = 2$	$r =$	± 1	± 3	± 4	± 5		± 9		± 12	± 13	± 14	± 15
$n = 3$	$r =$	± 1	± 3			± 8	± 9	± 11				
$n = 5$	$r =$	± 1						± 11		± 13	± 14	
$n = 6$	$r =$	± 1	± 3				± 9					
$n = 4$	$r =$	$+1$	-3	-4	-5		$+9$		$+12$	$+13$	-14	$+15$
$n = 10$	$r =$	± 1								± 13	± 14	
$n = 12$	$r =$	$+1$	-3				$+9$					
$n = 15$	$r =$	± 1						± 11				

$n = 2$	$r =$	± 16	± 19	± 20		± 22			± 25	± 27		
$n = 3$	$r =$			± 20			± 23	± 24		± 27	± 28	
$n = 5$	$r =$				± 21							± 29
$n = 6$	$r =$			± 20						± 27		
$n = 4$	$r =$	$+16$	-19	$+20$		$+22$			$+25$	-27		
$n = 10$												
$n = 12$	$r =$			$+20$						-27		

Schon hieraus lässt sich vermuthen, dass jede Congruenz vom Qten Grade (Q ist natürlich ein Factor von π) sich auf so viele Hülfscongruenzen, deren Gradexponenten respective

$$a^\alpha \quad b^\beta \quad c^\gamma \quad \ldots\ldots \quad l^\lambda$$

sind, zurückführen lasse, als überhaupt von einander verschiedene Primfactoren in Q hineingehen.

Bilden wir uns, um diese Vermuthung zu rechtfertigen, das System der Hülfscongruenzen:

$$\left.\begin{array}{l} A^{a^\alpha} \equiv r \\ B^{b^\beta} \equiv A \\ C^{c^\gamma} \equiv B \\ \ldots\ldots \\ \ldots\ldots \\ L^{l^\lambda} \equiv K \end{array}\right\} \pmod{P},$$

so lässt sich darthun, dass dasselbe der gegebenen Congruenz

$$x^Q = x^{a^\alpha b^\beta \ldots l^\lambda} \equiv r \pmod{P}$$

als vollkommen gleichgeltend betrachtet werden darf. In der That folgt durch allmählige Substitution jeder Hülfscongruenz in die nachfolgende:

$$\left.\begin{array}{l} A^{a^\alpha} \equiv r \\ B^{a^\alpha b^\beta} \equiv r \\ C^{a^\alpha b^\beta c^\gamma} \equiv r \\ \ldots\ldots \\ K^{a^\alpha \ldots k^\kappa} \equiv r \\ L^{a^\alpha \ldots l^\lambda} \equiv r \end{array}\right\} \pmod{P}$$

ablesen lässt und kann das Geschäft de· ·d, so ist
sich zusammenstellen:

r	1				
R''	1		−1		3
R'	1	−1	27	−27	1
$x \equiv R =$	+1	27	10	22	
	−1	−27	−10	−22	

·ung ist erfüllt,

r	8		
R''	9		−9
R'	3	−3	8
$x \equiv R =$	21	17	9
	−21	−17	−9

r	−9	
R''	8	
R'	9	−9
$x \equiv R =$	3	8
	−3	−8

·n dasselbe lässt sich vermöge der
·olgt umschreiben:

d) Aus dem
nent sich irgendw

$$r^{\frac{\pi}{a^\alpha}} \equiv 1$$

die Reste der
Exponenten

$$\equiv r^{\frac{\pi}{a^\alpha b^\beta}} \equiv 1$$

. . . .

bezüglichen
schiedene·
wieder ·
zwar w·

$$B^{a^\alpha b^\beta \frac{\pi}{a^\alpha b^\beta c^\gamma}} \equiv r^{\frac{\pi}{a^\alpha b^\beta c^\gamma}} \equiv 1$$

$$K^{a^\alpha b^\beta \dots k^\kappa \frac{\pi}{a^\alpha b^\beta \dots l^\lambda}} \equiv r^{\frac{\pi}{a^\alpha b^\beta \dots l^\lambda}} \equiv 1$$

·nd in dieser Form erkennt man die einzelnen Congruenzen sämmtlich
·als Potenzen der letzten Congruenz, die man auch schreiben kann

$$r^{\frac{\pi}{Q}} \equiv 1 \ (mod\ P),$$

und diese muss Gültigkeit haben, weil sonst r kein Rest der Qten Potenz und die vorgelegte Congruenz widersprechend wäre.

Die Rechnung ist ohne alle Schwierigkeit und ihr Gang, beispielsweise für die 12te und 30te Potenz durchgeführt, wird aus folgender schematischer Darstellung erhellen, bei welcher die den verschiedenen

…r zweiten, dritten, vierten und fünften Potenz zugehörigen Reste …sstabelle von §. 13 entnommen sind:

$$\equiv +1 \;-3 \;+9 \;+20 \;-27 \pmod{61}.$$

+1		—3			
—11	—1	20	24	—24	—20
11 21 29	14 —13 —1	12 15 —27	8 10 —18	18 —10 —8	27 —15 —12

+9			+20			
—7	—27	—8	3	28	—28	—3
3 19 —22	22 —19 —3	28 —26 —2	4 5 —9	23 —17 —6	6 17 —23	9 —5 —4

r	—27			
A	9	23	—23	—9
$x \equiv B$	16 20 25	—30 —24 —7	7 24 30	—25 —20 —16

$$x^{30} \equiv 1 \pmod{61}.$$

r	1					
A	+1			—1		
B	+1	+13	—14	+14	—13	—1
$x \equiv C$	1 9 20 —27 —3	12 25 —19 —14 —4	13 15 16 22 —5	5 —22 —16 —15 —13	4 14 19 —25 —12	3 27 —20 —9 —1

e) Auf den vorhergehenden Erörterungen beruht eine Methode, die primitiven Wurzeln eines Moduls und überhaupt die irgend einem Exponenten zugehörigen Zahlen zu finden, welche dadurch bemerkenswerth ist, dass sie gleichmässig die Fälle

$$P = p,\; p^n,\; 2p^n$$

umfasst.

Bezeichnen wir irgend einen Theiler von π mit Q, setzen, wie gewöhnlich,

$$\pi = QQ'$$

und bilden uns alle diejenigen Vielfachen von Q', welche in π aufgehen, sowie die Reste der Potenzen, welche diesen Vielfachen entsprechen: dann gehören alle diejenigen Zahlen der ersten Restreihe, welche in den folgenden nicht vorkommen, nach dem Modul P zu dem Exponenten Q.

Der Beweis ist sehr einfach. Da ein solcher übrig gebliebener Rest r in der ersten Reihe enthalten ist und in den übrigen fehlt, so ist er ein Rest der Q'ten Potenz und keiner höheren, deren Exponent ein Viel-

fachen von Q' ist. Daraus folgt, dass er nothwendig der Bedingungscongruenz

$$r^{\frac{\pi}{Q'}} \equiv r^{Q} \equiv 1 \ (mod\ P)$$

Genüge leistet und gleichzeitig kein Exponent existirt, der, ein Theiler von Q und kleiner als diese Zahl, die zugehörige Potenz von r der Einheit congruent machen könnte. Denn wäre ein solcher Exponent, etwa $\frac{Q}{m}$ möglich, so würde folgen, dass r ein Rest der $\left(\pi : \frac{Q}{m}\right) = (mQ')$ten Potenz wäre, was nach der Voraussetzung unzulässig ist.

Suchen wir z. B. die dem Exponenten 20 nach dem Modul 25 zugehörigen Zahlen, d. h. die primitiven Wurzeln von 25, so ist

$$P = 5^2,\ \pi = 20,\ Q' = 1,\ Q = 20$$

und die Vielfachen von Q', die in Betracht kommen, sind zunächst die sämmtlichen Theiler von 20, also:

$$1 \quad 2 \quad 4 \quad 5 \quad 10 \quad 20;$$

da aber die Reste der 4ten, 10ten und 20ten Potenz auf jeden Fall in denen der zweiten Potenz mit vorkommen, so brauchen wir nur die Reste der ersten, zweiten und fünften Potenz zu untersuchen. Diese Reste sind folgende:

$$r^1 \equiv \pm 1 \ \pm 2 \ \pm 3 \ \pm 4 \ \pm 6 \ \pm 7 \ \pm 8 \ \pm 9 \ \pm 11 \ \pm 12$$
$$r^2 \equiv \pm 1 \qquad \pm 4 \ \pm 6 \qquad \pm 9 \ \pm 11$$
$$r^5 \equiv \pm 1 \qquad \pm 7$$

Die Reste der ersten Reihe, die in der zweiten und dritten Reihe nicht vorkommen, sind:

$$\pm 2 \quad \pm 3 \quad \pm 7 \quad \pm 8$$

und man bekommt also, wenn man die kleinsten positiven Zahlen nimmt, in Uebereinstimmung mit den früheren Resultaten, folgende primitiven Wurzeln:

$$2 \quad 3 \quad 7 \quad 8 \quad 17 \quad 18 \quad 22 \quad 23.$$

Um auch ein Beispiel für den Modul $2p^n$ zu haben, wollen wir die zu dem Exponenten 10 nach dem Modul 50 gehörigen Zahlen uns berechnen. Man hat alsdann

$$P = 50,\ \pi = 20,\ Q = 10,\ Q' = 2$$

und die Vielfachen von Q', die in 20 aufgehen, sind:

$$2,\ 4,\ 10,\ 20;$$

da indessen die Reste der 20ten Potenz zugleich Reste der 10ten Potenz sind und also wegen derselben in der ersten Reihe keine Reste auszuschliessen sind, die nicht bereits ausgeschlossen wären, so brauchen wir blos die zweite, vierte und zehnte Potenz zu betrachten. Die Reihe der Zahlen, von denen wir die genannten Potenzen aus zu bilden haben, ist:

$$\pm 1 \quad \pm 3 \quad \pm 7 \quad \pm 9 \quad \pm 11 \quad \pm 13 \quad \pm 17 \quad \pm 19 \quad \pm 21 \quad \pm 23$$

und wir bekommen durch allmählige Potenzirung leicht folgende Reste:

$$r^2 \equiv \pm 1 \quad \pm 9 \quad \pm 11 \quad \pm 19 \quad \pm 21$$

$$r^4 \equiv +1 \quad -9 \quad +11 \quad -19 \quad +21$$

$$r^{10} \equiv \pm 1$$

Die gesuchten Zahlen, die zu dem Exponenten 10 nach dem Modul 50 gehören, sind mithin:

$$9 \quad 19 \quad -21 \quad -11.$$

Mit den vorstehenden Erörterungen ist der Beweis geliefert, dass jede Congruenz von der Form

$$x^Q \equiv r \ (mod\ P),$$

deren Exponent ein zusammengesetzter Theiler von π ist, sich immer auf eine beschränkte Anzahl solcher Congruenzen zurückführen lässt, deren Exponenten einfache Primfactoren von π sind. Wie wir wissen kommt man immer auf eine Congruenz solcher Art zurück, wenn man die allgemeinere Congruenz

$$x^N \equiv r \ (mod\ P),$$

wo P eine der drei Formen

$$p, \ p^n, \ 2p^n$$

hat, auflösen soll. Mithin erhellt, dass unser allgemeines Problem, wenn es in jedem einzelnen Falle ohne Probiren und vermittelst strenger Methode gelöst werden soll, im Allgemeinen folgende Daten als aus irgend welchen Tabellen entnehmbar voraussetzt:

A) Wenigstens eine, am passendsten die kleinste, primitive Wurzel des Moduls P, sowie zu jedem Theiler von π wenigstens eine ihm zugehörige Zahl.

B) Die Reste r jeder solchen Potenz, deren Exponent ein Primfactor von π ist, und zu jedem Reste wenigstens einen Zahlenwerth der Grösse x, durch welche er erzeugt wird.

In Crelle's schon einmal angeführter encyclopädischer Darstellung der Zahlentheorie befindet sich eine solche Tabelle für alle Primzahlen von 3 bis 101 und zwar geht dieselbe über die angegebene Beschränkung hinaus, indem zu jedem Exponenten alle zugehörigen Zahlen und zu jedem Reste x alle zugehörigen Werthe von x verzeichnet sind. Aber dagegen haben die Modul von der Form

$$p^n,\ 2p^n$$

keine Berücksichtigung gefunden, während doch wenigstens für die erstere Form dies sehr wünschenswerth sein dürfte.

5) Wir müssen, um alle möglichen Fälle zu erschöpfen, noch einen Fall der Congruenz

$$x^N \equiv r \pmod{p^n}$$

besonders betrachten, dies ist der Fall

$$p = 2,$$

und diese Untersuchung wird nicht schwer fallen, wenn wir auf die am Schlusse von Nr. 3 befindlichen diesen Fall betreffenden Erörterungen Bezug nehmen.

Zunächst können wir unmittelbar der allgemeinen Betrachtung folgenden Satz entnehmen, dessen Beweis durch die Natur des jetzigen Moduls nicht wesentlich modificirt wird:

a) W e n n N e i n e u n g e r a d e Z a h l i s t, s o h a t d i e C o n g r u e n z

$$x^N \equiv r \pmod{2^n}$$

n u r e i n e e i n z i g e A u f l ö s u n g, w e l c h e, i n d e m

$$q = 2^\lambda$$

d e n z u r g e h ö r i g e n E x p o n e n t e n b e z e i c h n e t, v e r m ö g e d e r b e i d e n C o n g r u e n z e n

$$Nz \equiv 1 \pmod{q}$$
$$x \equiv r^z \pmod{2^n}$$

s i c h b e s t i m m t.

Wenn dagegen N eine gerade Zahl und die Zahl $q = 2^\lambda$ der grösste gemeinschaftliche Theiler zwischen π und N ist, so bringe man die gegebene Congruenz auf die Form

$$(x^q)^{\frac{N}{q}} \equiv r \pmod{2^n}$$

und es erhellt, da $\frac{N}{q}$ nach der Voraussetzung ungerade sein muss, dass

dieselbe dann immer nach x^q eine, wie wir gezeigt haben, bestimmbare Auflösung und sonst keine mehr hat; möge dieselbe

$$x^q \equiv p \ (mod\ 2^n)$$

sein, so ist diese letzte Congruenz mit der gegebenen vollkommen identisch.

Beginnen wir mit dem einfachsten Falle

$$x^q \equiv 1 \ (mod\ 2^n),$$

in welchem $\varrho = 1$ angenommen wird, so ist evident, dass dieser Congruenz alle Zahlenwerthe x genügen müssen, welche zu dem Exponenten q oder zu einem niedrigeren Exponenten gehören und sonst keine mehr. Die übrig bleibenden ungeraden Zahlen von 1 bis 2^n sind dadurch ausgeschlossen, dass sie erst zu höheren Potenzen der Einheit gleich werden.

Um also die Anzahl sämmtlicher Wurzeln zu finden, müssen wir zuvor die Anzahl der zu irgend einem Exponenten gehörigen Zahlen kennen. Nun wissen wir, zu dem Exponenten 2^{n-x} gehören alle Zahlen von der Form:

$$2^x h \pm 1;$$

mithin haben die zu dem Exponenten 2^x gehörigen Zahlen die Form

$$2^{n-x} h \pm 1,$$

wo für h der Reihe nach die ungeraden Zahlen

$$1 \ 3 \ 5 \ 7 \ 9 \ldots\ldots 2^x - 1$$

einzusetzen sind; weiter darf man nicht gehen, denn schon für

$$h = 2^x + 1$$

erhielte man eine ungerade Zahl, die grösser als 2^n und irgend einer früheren congruent wäre. Hierdurch bekommen wir 2^{x-1} Paare von Zahlen, also überhaupt 2^x Zahlen, die dem Exponenten 2^n zugehören. Dies Raisonnement ist nur für die beiden Fälle

$$x = 0, 1$$

ungültig. Es lässt sich aber leicht zeigen, dass, wenn $x = 0$, 1 die einzige Zahl ist, welche zu dem Exponenten 1 gehört, dagegen, wenn $x = 1$, 3 Zahlen, nämlich:

$$-1,\ 2^{n-1}+1,\ 2^{n-1}-1.$$

Hiernach ist die Anzahl der sämmtlichen Wurzeln der Congruenz, welche uns zuletzt beschäftigte,

$$1 + 3 + 2^2 + 2^3 + 2^4 + \ldots\ldots + 2^\lambda = 1 + (1 + 2 + 2^2 + \ldots\ldots + 2^\lambda)$$

oder, wenn wir die bekannte Summenformel für eine geometrische Progression anwenden, deren Anfangsglied und Endglied gegeben sind,

$$=1+\frac{2^{\lambda+1}-1}{2-1}=2^{\lambda+1}.$$

Seien dieselben alle in der Reihe

$$1 \quad h' \quad h'' \quad h''' \ldots\ldots\ldots -1$$

enthalten, so sind die Wurzeln der allgemeineren Congruenz

$$x^q \equiv \varrho \ (mod\ 2^n),$$

wenn eine derselben, etwa

$$x \equiv H \ (mod\ 2^n)$$

bekannt ist, sämmtlich in der $(2^{\lambda+1})$gliedrigen Reihe

$$H \quad Hh' \quad Hh'' \quad Hh''' \ldots\ldots -H$$

inbegriffen. Denn es kann ohne Schwierigkeit gezeigt werden, eben sowohl, dass jedes Glied der vorgelegten Congruenz genügt, als auch, dass keine von ihnen allen verschiedene Zahl existire, von der das Gleiche gilt. Mithin können wir jetzt folgendes Theorem aussprechen:

b) Wenn 2^λ der grösste gemeinschaftliche Theiler zwischen N und $\pi=2^{n-2}$ ist, so ist die Congruenz

$$x^N \equiv r \ (mod\ 2^n)$$

identisch mit dem System der beiden Congruenzen:

$$\left.\begin{array}{l} \left(x^{2^\lambda}\right)^{\frac{N}{2^\lambda}} \equiv r \\ x^{2^\lambda} \equiv \varrho \end{array}\right\} (mod\ 2^n).$$

c) Die Congruenz

$$x^{2^\lambda} \equiv \varrho \ (mod\ 2^n),$$

wofern sie überhaupt möglich ist, hat $2^{\lambda+1}$ Lösungen, welche sämmtlich erhalten werden, wenn man eine willkürliche darunter mit den $2^{\lambda+1}$ Lösungen der Congruenz

$$x^{2^\lambda} \equiv 1 \ (mod\ 2^n)$$

durch Multiplication zusammensetzt.

Beispiel. Es sei die Congruenz

$$x^{12} \equiv -15 \ (mod\ 32),$$

gegeben. Man schreibe dieselbe sich um, wie folgt

$$(x^4)^3 \equiv -15$$

und löse sie nach x^4 vermittelst der Hülfscongruenzen

$$3z \equiv 1 \ (mod\ 2)$$

$$x^4 \equiv (-15)^z \ (mod\ 32)$$

auf. Dadurch wird die gegebene Congruenz auf die folgende mit ihr gleichgeltende zurückgebracht:

$$x^4 \equiv -15 \ (mod\ 32),$$

von der eine Auflösung durch Probiren gleich 11 gefunden wird. Diese Lösung multiplicire man mit den sämmtlichen Lösungen

$$\xi \equiv \pm 1 \ \pm 7 \ \pm 9 \ \pm 19$$

der Congruenz

$$\xi^4 \equiv 1 \ (mod\ 32),$$

so ergeben sich die sämmtlichen gesuchten Wurzelwerthe x, nämlich

$$x \equiv \pm 11 \ \pm 13 \ \pm 15 \ \pm 5$$

oder, wenn man nach der Grösse ordnet:

5 11 13 15 17 19 21 27.

In obiger Theorie ist noch ein Mangel. Indem sie schliesslich voraussetzt, dass wenigstens eine Wurzel der vorgelegten Congruenz durch Versuche bestimmt werde, sagt sie nichts davon, in wiefern dies Probiren überhaupt Aussicht auf Erfolg habe. Hier gilt nun im theilweisen Widerspruche zur allgemeinen Theorie der folgende Satz:

Wenn die Congruenz

$$x^{2^\lambda} \equiv \varrho \ (mod\ 2^n)$$

möglich ist, muss nothwendig die Congruenz

$$\varrho^{\frac{\pi}{2^\lambda}} = \varrho^{n-\lambda-2} \equiv 1 \ (mod\ 2^n)$$

bestehen und es können daher nur solche Zahlen, welche der letztgenannten Congruenz genügen, Reste der (2^λ)ten Potenz sein; aber es ist umgekehrt nicht unbedingt nothwendig, dass jede solche Zahl ein Rest der (2^λ)ten Potenz ist, sondern unter den $2^{n-\lambda-1}$ Lösungen der zuletzt erwähnten Potenz sind nur die Hälfte Reste und die übrig bleibenden Nichtreste.

Der erste Theil dieses Satzes beweist sich ohne Zuziehung eigenthümlicher Betrachtungen. Was die Umkehrung anbetrifft, so kann man wieder ohne alle Schwierigkeit den Nachweis führen, dass, wenn man in

den Ausdruck

$$x^{2^\lambda}$$

für x nach und nach die Zahlen der (2^{n-1})gliedrigen Reihe

$$1 \quad 3 \quad 5 \quad 7 \ldots\ldots 2^n - 1$$

substituirt, man

$$\frac{2^{n-1}}{2^{\lambda+1}} = 2^{n-\lambda-2}$$

verschiedene Reste und jedem Reste $2^{\lambda+1}$ verschiedene Zahlenwerthe des x als entsprechend bekommt. Nun sind alle diese Reste unter den $(2^{n-\lambda-1})$ Lösungen der Congruenz

$$\varrho^{n-\lambda-2} \equiv 1 \; (mod\; 2^n)$$

enthalten; also besteht offenbar die eine Hälfte dieser Lösungen aus lauter Resten, die andere aus lauter Nichtresten der (2^λ)ten Potenz.

Was die Unterscheidung derjenigen Wurzeln, welche Reste, von denjenigen, welche Nichtreste sind, betrifft, so kann man zunächst bemerken, dass die Gesammtmenge der Wurzeln offenbar die Anordnung in $(2^{n-\lambda-2})$ Gruppen zu je 2 Zahlen der Form

$$+\varrho, -\varrho$$

gestattet und, dass immer eine unter diesen beiden Zahlen ein Rest, die andere ein Nichtrest ist. Wären nämlich beide zu gleicher Zeit Reste, so beständen für irgend welche bestimmbare x und y die Congruenzen

$$\left.\begin{array}{l} x^{2^\lambda} \equiv \varrho \\ y^{2^\lambda} \equiv -\varrho \end{array}\right\} (mod\; 2^n)$$

und aus ihnen folgte durch Subtraction

$$x^{2^\lambda} - y^{2^\lambda} \equiv 2\varrho \; (mod\; 2^n),$$

also, wofern man, wie wir im Folgenden immer thun wollen, $n \geqq 3$ annimmt,

$$x^{2^\lambda} - y^{2^\lambda} \equiv 2\varrho \; (mod\; 4).$$

Nun ist die linke Seite dieser Congruenz theilbar durch $x^2 - y^2$ (denn λ ist immer eine von 0 verschiedene positive Zahl) und, da x und y ungerade, mithin $x^2 - y^2$ ein Vielfaches von 4 ist, darum auch theilbar durch 4, d. h.

$$x^{2^\lambda} - y^{2^\lambda} \equiv 0 \; (mod\; 4).$$

Die Vergleichung dieser beiden Congruenzen liefert:

$$2\varrho \equiv 4 \; (mod\; 4)$$

also

$$\varrho \equiv 2 \pmod 2,$$

d. h. ϱ müsste eine gerade Zahl sein, welches sich im Widerspruche zu seiner Bestimmung befindet. Mithin können die Zahlen $+\varrho$ und $-\varrho$ nicht beide Reste sein.

Ebensowenig können sie beide Nichtreste sein. Denn in diesem Falle würden noch $(2^{n-\lambda-2}-1)$ Paare von Wurzeln übrig bleiben und darunter könnten sämmtliche $2^{n-\lambda-2}$ Reste nur so enthalten sein, dass wieder die Zahlen wenigstens einer Gruppe beide Reste wären. Wir kämen also auf denselben Widerspruch wie vorhin.

Wir bemerken weiter, dass man die Wurzeln, wenn man $+1$ und -1 ausschliesst (von denen $+1$ ein Rest, -1 ein Nichtrest ist), auch noch in einer anderen Weise gruppiren kann, nämlich so, dass immer je zwei Wurzeln von der Form

$$2^{\varkappa}h+1, \; 2^{\varkappa}h-1$$

als zusammengehörige betrachtet werden. Die verschiedenen Werthe, welche hier h annehmen kann, sind

$$h = 1 \;\; 3 \;\; 5 \;\; 7 \; \ldots . \; 2^{n-\varkappa}-1$$

und die verschiedenen Werthe, deren $\varkappa$ fähig ist:

$$\varkappa = n-1 \;\; n-2 \;\; n-3 \; \ldots . \; \lambda+2.$$

Es gilt nun wieder der nämliche Satz, wie früher, dass die Zahlen je einer Gruppe zu gleicher Zeit beide weder Reste noch Nichtreste sein können.

Sie können zunächst nicht beide Reste sein; denn dann wären die Congruenzen

$$\left.\begin{aligned} x^{2^\lambda} &\equiv 2^{\varkappa}h+1 \\ y^{2^\lambda} &\equiv 2^{\varkappa}h-1 \end{aligned}\right\} \pmod{2^n}$$

möglich und es würde durch Addition folgen:

$$x^{2^\lambda}+y^{2^\lambda} \equiv 2^{\varkappa-1}h \pmod{2^n},$$

was nicht angeht, weil x, y, h ungerade Zahlen und folgeweise die linke Seite der Congruenz gerade, die rechte dagegen ungerade ausfällt. — Dass beide Zahlen zu gleicher Zeit nicht Nichtreste sein können, lässt sich so wie eben vorher nachweisen.

Wir sprechen die gewonnenen Resultate in folgendem Theoreme aus:

Je zwei zusammengehörige Wurzeln der Bedingungs-congruenz

$$\varrho^{2^{n-\lambda-2}} \equiv 1 \ (mod\ 2^n),$$

die entweder die Form

$$+\varrho,\ -\varrho$$

oder die Form

$$2^{\varkappa}h+1,\ 2^{\varkappa}h-1$$

haben, können nicht zugleich weder Reste noch Nichtreste der (2^{λ})ten Potenz sein.

Dieser Satz reicht zwar nicht aus, um ohne alle Versuche diejenigen Wurzeln, welche Reste sind, von denen, die Nichtreste sind, zu sondern; aber er beschränkt immerhin die Anzahl der Versuche bedeutend und findet daher die nützlichste Anwendung bei der Bestimmung von Potenzresten nach dem Modul 2^n. Wir werden weiter unten Gelegenheit haben die Art der Anwendung an einem Beispiele zu zeigen.

6) Betrachten wir endlich die Congruenz

$$Ax^N \equiv R \ (mod\ P),$$

wo A und R relative Primzahlen zu P und P einen willkürlich zusammengesetzten Modul bezeichnet, so lässt sich immer vermöge Auflösung der Congruenz

$$A\mu \equiv 1 \ (mod\ P)$$

ein Factor μ von der Beschaffenheit bestimmen, dass, wenn man die gegebene Congruenz mit ihm multiplicirt und darauf die Vielfachen von P abstreift, dieselbe auf die Form

$$x^N \equiv r \ (mod\ P)$$

kommt. Wenn dieser Congruenz irgend welche Zahlenwerthe von x Genüge leisten, so muss gleichzeitig das System der Congruenzen

$$x^N \equiv r \ (mod\ a^{\alpha})$$
$$x^N \equiv r \ (mod\ b^{\beta})$$
$$x^N \equiv r \ (mod\ c^{\gamma})$$
$$\cdots\cdots$$
$$\cdots\cdots$$

befriedigt werden und umgekehrt, wenn dies System von Congruenzen gleichzeitig besteht, so folgt aus ihm, da die Grössen a^{α}, b^{β}, c^{γ} ..... [illegible] Primzahlen unter einander sind, die gegebene Congruenz. Indem [illegible]genannten Congruenzen auflösen, erhalten wir Ausdrücke von

der Form

$$x \equiv \varrho' \ (mod\ a^{\alpha})$$
$$x \equiv \varrho'' \ (mod\ b^{\beta})$$
$$x \equiv \varrho''' \ (mod\ c^{\gamma})$$
$$\cdots\cdots$$
$$\cdots\cdots$$

und die Aufgabe ist mithin auf das bereits früher behandelte Problem zurückgebracht: Eine Zahl zu bestimmen, welche durch gegebene Divisoren dividirt gegebene Reste lässt. Sei die Anzahl der ϱ respective n', n'', n''', ..., so sind $n'n''n'''$...... von einander verschiedene Combinationen der Reste ϱ', ϱ'', ϱ'''......, möglich und eben so gross ist die Zahl der Lösungen, welche die gegebene Congruenz nach dem Modul P zulässt.

Indem wir näher auf das Detail der Ausführung eingehen, hat man zunächst nach §. 8 die Hülfscongruenzen

$$m'b^{\beta}c^{\gamma}d^{\delta} \ldots\ldots \equiv 1 \ (mod\ a^{\alpha})$$
$$m''a^{\alpha}c^{\gamma}d^{\delta} \ldots\ldots \equiv 1 \ (mod\ b^{\beta})$$
$$m'''a^{\alpha}b^{\beta}d^{\delta} \ldots\ldots \equiv 1 \ (mod\ c^{\gamma})$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$

aufzulösen und die daraus folgenden kleinsten Werthe von m', m'', m'''.... einzusetzen in den Ausdruck

$$\varrho \equiv \varrho' m' b^{\beta}c^{\gamma}d^{\delta} \ldots\ldots + \varrho'' m'' a^{\alpha}c^{\gamma}d^{\delta} \ldots\ldots + \varrho''' m''' a^{\alpha}b^{\beta}d^{\delta} \ldots + \ldots \ (mod\ P).$$

Die Congruenz

$$x \equiv \varrho \ (mod\ P)$$

repräsentirt alsdann, indem man in den Ausdruck für ϱ sich alle nur möglichen Werthe für ϱ', ϱ'', ϱ''', ... substituirt denkt, alle Lösungen der gegebenen Congruenz.

Machen wir die specielle Annahme

$$P = 72, \ a^{\alpha} = 3^2, \ b^{\beta} = 2^3;$$

dann sind die beiden Hülfscongruenzen nach m' und m''

$$8m' \equiv 1 \ (mod\ 9), \text{ also } m' = -1$$

und

$$9m'' \equiv 1 \ (mod\ 8), \text{ also } m'' = +1.$$

Die Substitution der Werthe von m' und m'' in ϱ giebt

$$\varrho \equiv -8\varrho' + 9\varrho'' \ (mod\ 72)$$

und es sind nur noch die verschiedenen Werthe zu bestimmen, welche hier für ϱ' und ϱ'' einzusetzen sind, eine Bestimmung, die wir in allgemeiner Form nicht leisten können, so dass wir, um die Rechnung weiter zu führen, genöthigt sind, den Grössen N und r irgend welche speciellen Werthe zu ertheilen. Nehmen wir daher die specielle Congruenz

$$11x^{20} \equiv -13 \ (mod\ 72)$$

an; dann findet man vermöge der Congruenz

$$11\mu \equiv 1 \ (mod\ 72)$$

den Factor

$$\mu = -13$$

von der Beschaffenheit, dass, wenn man die vorhergehende damit multiplicirt und darauf die Vielfachen von 72 abstreift, die einfachere Congruenz

$$x^{20} \equiv 25 \ (mod\ 72)$$

erhalten wird, welche sich sogleich in das System der beiden Congruenzen

$$x^{20} \equiv 25 \equiv -2 \ (mod\ 9)$$

und

$$x^{20} \equiv 25 \equiv 1 \ (mod\ 8)$$

zerlegt.

Was die auf den Modul 9 bezügliche Congruenz anbetrifft, so hat man

$$\pi = S'''9 = 6$$

und sie gestattet also eine Erniedrigung ihres Grades dadurch, dass man die Vielfachen von 6 im Exponenten abwirft. Dadurch geht sie über in

$$x^2 \equiv -2 \ (mod\ 9)$$

und man findet nun leicht die beiden in den kleinsten Zahlen ausgedrückten Wurzeln

$$\varrho' = +4, \ -4.$$

Die auf den Modul 8 bezügliche Congruenz, für welche

$$\pi = 2^{n-2} = 2$$

ist, hat dieselben reellen Wurzeln, wie die niedrigere Congruenz

$$x^2 \equiv 1 \ (mod\ 8),$$

nämlich die Zahlenwerthe

$$\varrho'' = 1, \ 3, \ -3, \ -1.$$

Substituiren wir die verschiedenen Werthe von ϱ' und ϱ'' in den Wurzelausdruck

$$\varrho \equiv -8\varrho' + 9\varrho'' \ (mod\ 72),$$

so erhalten wir folgende verschiedene Formen:

$$\varrho \equiv -8.4+9. \quad 1 \text{ und } 8.4+9. \quad 1$$
$$. \quad 3 \qquad . \quad 3$$
$$.-3 \qquad .-3$$
$$.-1 \qquad .-1$$

also, wenn man zusammenzieht, sind die verschiedenen möglichen Werthe für ϱ oder, was dasselbe ist, für x:

$$x \equiv -23 \; -5 \; 14 \; 31 \; -31 \; -14 \; 5 \; 23 \; (mod\; 72)$$

oder, wenn man nur positive Reste zulassen will und nach der Grösse ordnet:

$$x \equiv 5 \; 14 \; 23 \; 31 \; 41 \; 49 \; 58 \; 67 \; (mod\; 72).$$

Selbstverständlich können die Begriffe der primitiven Wurzeln und die damit verwandt sind, auch auf den vorliegenden Fall ausgedehnt werden. Da dies indessen für die Anwendung auf das Nachfolgende überflüssig ist, begnügen wir uns auszuführen, dass der Exponent, zu welchem eine primitive Wurzel gehört, nur in den abgehandelten speciellen Fällen

$$P = p^n, \; 2p^n$$

geradezu mit der Zahl

$$S'''P = \pi = a^{\alpha-1}(a-1)b^{\beta-1}(b-1)c^{\gamma-1}(c-1)\ldots.$$

zusammenfällt, in allen andern dagegen der kleinste gemeinschaftliche Dividuus μ zwischen den Zahlen

$$S'''a^\alpha, \; S'''b^\beta, \; S'''c^\gamma, \; \ldots.,$$

die wir der Kürze halber mit

$$A, \quad B, \quad C, \ldots.$$

bezeichnen, sein wird. Die Exponenten, welche zu den übrigen Zahlen x, die nicht primitive Wurzeln sind, gehören, müssen sämmtlich Theiler von μ sein und μ überhaupt in dem allgemeinen Probleme die nämliche Rolle spielen, wie π in den bisherigen Entwickelungen. (Sollte einer der Primfactoren von P, etwa a, gleich 2 sein, so ist das bezügliche A nicht geradezu $S'''a^\alpha$, sondern $\frac{1}{2}S'''a^\alpha$).

Um den Beweis zu führen, bemerken wir, dass, wenn x eine beliebige relative Primzahl zu dem Modul P bezeichnet, nothwendig die Congruenzen

$$x^A \equiv 1 \; (mod\; a^\alpha),$$
$$x^B \equiv 1 \; (mod\; b^\beta),$$
$$x^C \equiv 1 \; (mod\; c^\gamma)$$
$$\ldots\ldots$$
$$\ldots\ldots$$

statt haben. Vorausgesetzt nun, dass P nicht eine der beiden erwähnten Ausnahmeformen hat, werden die Zahlen A, B, C, ... alle einen gemeinschaftlichen Theiler besitzen, der keine niedrigere Potenz von 2 als die erste sein kann; also ist der kleinste gemeinschaftliche Dividuus μ mit Nothwendigkeit eine Zahl kleiner als $\pi = ABC\ldots$. Erheben wir jetzt die vorgenannten Congruenzen alle auf solche Potenzen, dass der Exponent von x gleich μ wird, so erkennt man, dass die μte Potenz jeder beliebigen Zahl x der Einheit congruent wird. Zu gleicher Zeit ist keine niedrigere Potenz nachweisbar, für welche gleichfalls alle Zahlen x dieser selben Congruenz genügen. Damit sind die Grundlagen, auf denen die gesammte Theorie der primitiven Wurzeln ruht, auch für einen Modul von beliebiger Beschaffenheit festgestellt.

Wir ziehen noch die weitere Folgerung, dass die auf irgend eine Zahl x bezügliche Restperiode

$$1 \quad x \quad x^2 \quad x^3 \quad \ldots\ldots \quad x^{\mu-1} \quad x^{\mu} \quad \ldots\ldots$$

höchstens μ von einander verschiedene Zahlen, also, da $\mu < \pi = S''' P$ ist, auf keinen Fall alle Zahlen enthalten kann, die kleiner als P und relative Primzahlen zu P sind. Sie wird genauer, wenn x eine primitive Wurzel von P ist, d. h. zu dem Exponenten μ gehört, μ von einander verschiedene Zahlen, dagegen, wenn x zu einem Theiler q von μ gehört, nur q von einander verschiedene Zahlen enthalten.

Wir wollen nicht specieller auf diesen Gegenstand eingehen und begnügen uns an einigen durchgeführten Beispielen dem Anfänger ein geeignetes Uebungsmaterial zu bieten.

$$x^N \equiv r \ (mod\ 15).$$

x	x^2	x^3	x^4
1	1	1	1
2	4	—7	1
4	1	4	1
7	4	—2	1
—7	4	2	1
—4	1	—4	1
—2	4	7	1
—1	1	—1	1

$x^N \equiv r \ (mod\ 120)$.

x	x^2	x^3	x^4	x	x^2	x^3	x^4
1				—59	1		
7	49	—17	1	—53	9	—43	1
11	1			—49	1		
13	49	37	1	—47	49	—23	1
17	49	— 7	1	—43	49	53	1
19	1			—41	1		
23	49	7	1	—37	49	—13	1
29	1			—31	1		
31	1			—29	1		
37	49	13	1	—23	49	— 7	1
41	1			—19	1		
43	49	—53	1	—17	49	7	1
47	49	23	1	—13	49	—37	1
49	1			—11	1		
53	49	—43	1	— 7	49	17	1
59	1			— 1	1		

$x^N \equiv r \ (mod\ 105)$.

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}
1											
2	4	8	16	32	—41	23	46	—13	—26	—52	1
4	16	—41	56	—26	1						
8	—41	—13	1								
11	16	—34	46	—19	1						
13	—41	— 8	1								
16	46	1									
17	—26	—22	46	47	—41	38	16	—43	4	—37	1
19	46	34	16	—11	1						
22	—41	43	1								
23	4	—13	16	—52	—41	2	46	8	—26	32	1
26	46	41	16	— 4	1						
29	1										
31	16	—29	46	—44	1						
32	—26	8	46	2	—41	—52	16	—13	4	23	1
34	1										
37	4	43	16	—38	—41	—47	46	22	—26	—17	1
38	—26	—43	46	—37	—41	17	16	—22	4	47	1
41	1										
43	—41	22	1								
44	46	29	16	—31	1						
46	16	1									
47	4	—22	16	17	—41	—37	46	—43	—26	38	1
52	—26	13	46	—23	—41	—32	16	— 8	4	— 2	1

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}
—52	—26	—13	46	23	—41	32	16	8	4	2	1
—47	4	22	16	—17	—41	37	46	43	—26	—38	1
—46	16	— 1	46	—16	1						
—44	46	—29	16	31	1						
—43	—41	—22	1								
—41	1										
—38	—26	43	46	37	—41	—17	16	22	4	—47	1
—37	4	—43	16	38	—41	47	46	—22	—26	17	1
—34	1										
—32	—26	— 8	46	— 2	—41	52	16	13	4	—23	1
—31	16	29	46	44	1						
—29	1										
—26	46	—41	16	4	1						
—23	4	13	16	52	—41	— 2	46	— 8	—26	—32	1
—22	—41	—43	1								
—19	46	—34	16	11	1						
—17	—26	22	46	—47	—41	—38	16	43	4	37	1
—16	46	— 1	16	—46	1						
—13	—41	8	1								
—11	16	34	46	19	1						
— 8	—41	13	1								
— 4	16	41	46	26	1						
— 2	4	— 8	16	—32	—41	—23	46	13	—26	52	1
— 1	1										

Die Anzahl der relativen Primzahlen zu 105, d. h. der Zahlengrössen x in der letzten Tabelle, ist

$$S'''P = S'''(3.5.7) = 48,$$

die Grösse μ dagegen ist der kleinste gemeinschaftliche Dividuus zwischen $S'''3$, $S'''5$ und $S'''7$, hieraus folgt

$$\mu = 12.$$

Die verschiedenen Zahlengrössen vertheilen sich, wie folgt, auf die einzelnen Divisoren von μ:

q	x							
1	1							
2	29	34	41	—41	—34	—29	—1	
3	16	46						
4	8	13	22	43	—43	—22	—13	—8
	4	11	19	26	31	44	—46	
6	—44	—31	—26	—19	—16	—11	—4	
	2	17	23	32	37	38	47	52
12	—52	—47	—38	—37	—32	—23	—17	—2

Um den Zusammenhang, der in den auf einen zusammengesetzten Modul bezüglichen Zahlenverhältnissen herrscht, näher hervorzuheben, mögen folgende Bemerkungen dienen, die wir ohne Beweis hinstellen:

Wenn irgend ein Exponent q das Product von mehreren Exponenten q', q'', q''', ... ist, die unter einander relative Primzahlen sind, so erhält man die zu q gehörigen Zahlen, wenn man die respective zu q', q'', q''', ... gehörigen Zahlen mit einander durch Multiplication combinirt; ihre Menge ist daher gleich dem Producte derjenigen Zahlen, welche anzeigen, wie viele x respective zu den Exponenten q', q'', q''', ... gehören.

Hiernach kommt es blos darauf an, die zugehörigen Zahlen zu allen solchen Theilern von μ zu finden, welche Potenzen irgend eines in μ vorkommenden Primfactors und relative Primzahlen zu den übrigen in μ vorkommenden Primfactoren sind.

Sei ein solcher Theiler $\varkappa$ und die Wurzeln der Congruenzen

$$x^\varkappa \equiv 1 \ (mod\ a^\alpha,\ b^\beta,\ c^\gamma,\ ....)$$

respective

$$\begin{matrix} A' & A'' & A''' & A'''' \ .... \\ B' & B'' & B''' & B'''' \ .... \\ C' & C'' & C''' & C'''' \ .... \end{matrix}$$

dann können die Wurzeln der Congruenz

$$x^\varkappa \equiv 1 \ (mod\ P)$$

bekanntlich vermöge der Grössen A, B, C bestimmt werden. Unter diesen Wurzeln gehören nun alle diejenigen nicht zu dem Exponenten $\varkappa$, welche zu Factoren lauter solche Zahlen haben, die nicht zu dem Exponenten $\varkappa$ nach den gleichnamigen Moduln

$$a^\alpha \quad b^\beta \quad c^\gamma \ ....$$

gehören; dagegen gehören alle die zu dem Exponenten $\varkappa$, deren Factoren entweder alle oder zum Theil dem Exponenten q nach den gleichnamigen Moduln zugehören.

Sei die Anzahl der Wurzeln, welche die genannten Congruenzen nach den Moduln a^α, b^β, c^γ, ... haben, dargestellt respective durch die Zahlensymbole

$$(a),\ (b),\ (c),\ ....$$

und die Anzahl derjenigen unter diesen Wurzeln, welche nicht zu dem Exponenten $\varkappa$ nach dem gleichnamigen Modul gehören, in ähnlicher Weise

durch die Formen

$$(\alpha),\ (\beta),\ (\gamma),\ \ldots.$$

symbolisirt, so ist die Anzahl der zu dem Exponenten $\varkappa$ nach dem Modul P gehörigen Zahlen ausgedrückt durch die Differenz

$$(a).(b).(c)\ \ldots\ldots\ -(\alpha).(\beta).(\gamma)\ \ldots\ldots$$

Es kann hierbei vorkommen, dass einige der Factoren des ersten Gliedes gleich werden den gleichnamigen Factoren des zweiten Gliedes; also z. B. es kann möglicher Weise (a) gleich (α) werden und dieser Fall wird immer eintreten, wenn $\varkappa$ kein Theiler von $S'''a^\alpha$ (oder respective, wenn $a=2$, von $\frac{1}{2}S'''a^\alpha$) ist: aber niemals, bei der über $\varkappa$ gemachten Voraussetzung, können alle Factoren beider Producte einander gleich und der Werth der Differenz gleich 0 werden.

Nehmen wir z. B.

$$P=120,\quad \varkappa=2$$

an, dann sind die in Betracht kommenden Congruenzen die folgenden drei:

$$x^2\equiv 1\ (mod\ 8,\ 3,\ 5)$$

und die Zahl der Lösungen ist respective

$$(a)=4,\ (b)=2,\ (c)=2,$$

sowie die Zahl der nicht zu dem Exponenten 2 gehörigen Wurzeln respective

$$(\alpha)=1,\ (\beta)=1,\ (\gamma)=1;$$

mithin folgt die Zahl der zu 2 nach dem Modul 120 gehörigen Combinationsproducte aus den verschiedenen Wurzeln dieser Congruenzen, gleich der Differenz

$$4.2.2-1.1.1=15.$$

Diese 15 Zahlen sind zu Folge der auf den Modul 120 bezüglichen Tabelle:

11 19 29 31 41 49 59 —59 —49 —41 —31 —29 —19 —11 —1.

Behalten wir nun den Modul 120 bei, nehmen aber $\varkappa=4$ an, so sind die drei Congruenzen, die in Betracht kommen:

$$x^4\equiv 1\ (mod\ 8),\ x^4\equiv 1\ (mod\ 3),\ x^4\equiv 1\ (mod\ 5).$$

Die erste hat, da $\pi=2$ ist und 2 der grösste Theiler, den π mit 4 gemeinschaftlich hat, 4 Wurzeln, unter denen aber keine zu dem Exponenten 4 gehören kann; die zweite hat aus ähnlichen Gründen (denn $\pi=S'''3=2$) 2 Wurzeln, unter denen gleichfalls keine dem Exponenten 4 zugehört; die letzte endlich hat 4 Wurzeln und darunter gehören $S'''4=2$ zu dem Exponenten 4; mithin ist

$$(a) = 4, \ (\alpha) = 4, \ (b) = 2, \ (\beta) = 2, \ (c) = 4, \ (\gamma) = 2$$

ıd die Menge der zu 4 nach dem Modul 120 gehörigen Zahlen gleich

$$4 . 2 . 4 - 4 . 2 . 2 = 16,$$

Uebereinstimmung mit der Tabelle, aus der sich diese Zahlen, wie lgt, ergeben:

7	13	17	23	37	43	47	53
—53	—47	—43	—37	—23	—17	—13	—7.

Nehmen wir als letztes Beispiel

$$P = 105, \ \varkappa = 3,$$

ınn sind die drei aufzulösenden Congruenzen

$$x^3 \equiv 1 \ (mod\ 3), \ x^3 \equiv 1 \ (mod\ 5), \ x^3 \equiv 1 \ (mod\ 7)$$

ıd man findet

$$(a) = 1, \ (\alpha) = 1, \ (b) = 1, \ (\beta) = 1, \ (c) = 3, \ (\gamma) = 1,$$

ithin

$$(a) . (b) . (c) - (\alpha) . (\beta) . (\gamma) = 1 . 1 . 3 - 1 . 1 . 1 = 2.$$

Der specielle Fall $\varkappa = 2$ eignet sich zu einer allgemeineren Betrachng. Sei n die Menge der ungleichen Primfactoren, welche in P hineinıhen, so ist die Anzahl der Wurzeln, welche die Congruenz

$$x^2 \equiv 1 \ (mod\ P)$$

ıt, 2^n, wenn die Primfactoren von P alle ungerade sind, dagegen 2^{n+1}, enn eine darunter gleich 2 ist; mithin ist im ersten Falle

$$2^n - 1,$$

ı zweiten dagegen

$$2^{n+1} - 1$$

e Menge der Zahlen, welche zu dem Exponenten 2 nach dem Modul P ıhören.

Dritter Abschnitt.

Von den quadratischen Resten und Nichtresten im Besonderen.

§. 15.

Begrenzung der Aufgabe.

1) Der Begriff der Benennung „quadratischer Rest oder Nichtrest" kann nach dem, was vorhergeht, keine Unklarheit mehr darbieten. Sei P irgend ein beliebig zusammengesetzter Modul,

$$P = 2^{\epsilon} a^{\alpha} b^{\beta} c^{\gamma} \ldots\ldots,$$

so wird eine Zahl R quadratischer Rest oder Nichtrest genannt, je nachdem die Congruenz

$$x^2 \equiv R \ (mod\ P)$$

möglich oder unmöglich ist. Hierbei betrachten wir nur solche Formen von A, welche relative Primzahlen zu P sind, also irgend einer der Zahlen

$$1 \ m' \ m'' \ m''' \ \ldots\ldots \ P-1$$

congruent sind. Es giebt allerdings quadratische Reste, welche mit P einen Theiler gemein haben können, so z. B. für jeden beliebigen Modul die Zahl 0 und alle damit congruenten. In gewissen Fällen können auch noch von 0 verschiedene Zahlen mit P einen Theiler gemeinschaftlich besitzen und doch quadratische Reste sein, wie z. B. die Zahlen

$$4 \ 9 \ 36$$

für den Modul 72. Aber ihre Bestimmung und Untersuchung ist immer äusserst einfach und kann daher zweckmässig für sich besonders vorgenommen werden, weil ihre Hereinziehung in die allgemeine Betrachtung nur dazu dienen würde, die Concinnität der Theoreme aufzuheben.

Wenn Q und Q' zwei relative Primzahlen zu einander sind, so ist die Congruenz

$$x^2 \equiv R \ (mod\ QQ')$$

identisch mit dem Systeme der beiden Congruenzen

$$x^2 \equiv R \ (mod\ Q) \quad x^2 \equiv R \ (mod\ Q');$$

denn einmal folgen aus der ersten die beiden letzten, und dann sind umgekehrt alle Zahlen x, welche die beiden letzten gleichzeitig befriedigen, auch Lösungen der ersten. Zu Folge der eingeführten Benennung erhalten wir mithin die beiden Theoreme:

Wenn eine Zahl zu zwei Moduln, die mit einander keinen Theiler ausser 1 gemeinschaftlich haben, quadratischer Rest ist, so ist sie auch zu dem Producte dieser Moduln quadratischer Rest.

Wenn eine Zahl quadratischer Rest zu den einzelnen Factoren

$$2^n \ a^\alpha \ b^\beta \ c^\gamma \ldots\ldots$$

des Moduls P ist, so ist sie auch ein quadratischer Rest des Moduls P selbst; sie ist dagegen Nichtrest von P, wenn sie es zu irgend einem der genannten Factoren ist.

Nach diesem letzten Theoreme muss R ein quadratischer Rest von P sein, wenn die Congruenzen

$$x^2 \equiv R \ (mod\ 2^n)$$
$$x^2 \equiv R \ (mod\ a^\alpha)$$
$$x^2 \equiv R \ (mod\ b^\beta)$$
$$x^2 \equiv R \ (mod\ c^\gamma)$$
. . . .
. . . .

für irgend welche bestimmten Zahlenwerthe von x (mögen dieselben nun für alle Congruenzen nach dem Modul P dieselben sein, oder für die verschiedenen Congruenzen verschieden ausfallen) möglich sind. Damit sie möglich sind, ist nothwendig, dass man gleichzeitig habe

$$R^{2^{n-3}} \equiv 1 \ (mod\ 2^n)$$
$$R^{\frac{1}{2}a^{\alpha-1}(a-1)} \equiv 1 \ (mod\ a^\alpha)$$
$$R^{\frac{1}{2}b^{\beta-1}(b-1)} \equiv 1 \ (mod\ b^\beta)$$
$$R^{\frac{1}{2}c^{\gamma-1}(c-1)} \equiv 1 \ (mod\ c^\gamma)$$
. . . .
. . . .

und zu gleicher Zeit ist das Bestehen dieser letzten Congruenzen, mit Ausnahme der ersten, auch ein vollkommen zureichender Grund, um respective auf die Möglichkeit der ihnen gleichnamigen unter den vorhergehenden Congruenzen schliessen zu dürfen. Was die erste, nämlich

$$R^{2^{n-3}} \equiv 1 \ (mod\ 2^n)$$

anbetrifft, so kann man nicht, wenn sie besteht, mit Endgültigkeit schliessen, dass die Congruenz

$$x^2 \equiv R \ (mod\ 2^n)$$

möglich sei; denn unter ihren Wurzeln, wie wir im vorhergehenden Paragraphen gesehen haben, liefert nur die Hälfte solche Zahlen R, für welche diese Möglichkeit eintritt. Seien diese Wurzeln, die offenbar in der Anzahl 2^{n-3} vorhanden sind,

$$L' \ L'' \ L''' \ L'''' \ldots\ldots;$$

ferner mögen die Wurzeln R der folgenden auf die Moduln a^α, b^β, c^γ, ... bezogenen Bedingungscongruenzen, die respective in der Anzahl

$$\tfrac{1}{2}a^{\alpha-1}(a-1), \ \tfrac{1}{2}b^{\beta-1}(b-1), \ \tfrac{1}{2}c^{\gamma-1}(c-1), \ldots\ldots$$

vorhanden sind, durch die Symbole

$$\begin{array}{llll} A' & A'' & A''' & A'''' \ldots \\ B' & B'' & B''' & B'''' \ldots \\ C' & C'' & C''' & C'''' \ldots \\ \ldots & \ldots & & \\ \ldots & \ldots & & \end{array}$$

dargestellt werden: dann sind die

$$L \ A \ B \ C \ldots$$

die sämmtlichen quadratischen Reste der bezüglichen Moduln

$$2^n \ a^\alpha \ b^\beta \ c^\gamma \ldots$$

und man findet zu Folge der in der letzten Nummer des vorhergehenden Paragraphen aufgestellten Principien die sämmtlichen Zahlen R, welche quadratische Reste zu P sind, indem man sich alle diejenigen Zahlen bestimmt, welche durch die Modul 2^n a^α, b^β, c^γ, ... dividirt bezüglich die Reste L, A, B, C, ... lassen. Demgemäss ist die Anzahl der R gleich dem Producte aus denjenigen Zahlen, welche respective die Menge der L, A, B, C, ... angeben, d. h. sie ist gleich

$$2^{n-3}.\tfrac{1}{2}a^{\alpha-1}(a-1).\tfrac{1}{2}b^{\beta-1}(b-1).\tfrac{1}{2}c^{\gamma-1}(c-1)\ldots\ldots$$
$$=\frac{1}{2.2.2.2\ldots\ldots}.\tfrac{1}{2}S'''2^n.S'''a^\alpha.S'''b^\beta.S'''c^\gamma\ldots\ldots$$
$$=\frac{1}{2.2.2.2\ldots\ldots}.\tfrac{1}{2}S'''P,$$

ıd es erhellt nun leicht folgendes Theorem:

Wenn der Modul P aus ν von einander verschiedenen rimfactoren sich irgend wie zusammensetzt (und der Factor , wenn er vorkommt, in einer höheren als der zweiten Potenz auftritt), o ist die Anzahl der sämmtlichen zu dem Modul P mögliben quadratischen Reste

$$\frac{1}{2^{\nu+1}}S'''P$$

nd näher, wenn P eine der Formen

$$p^n,\ 2p^n$$

at, gleich der halben Anzahl aller Zahlen, welche kleiner ls P und relative Primzahlen zu P sind; die übrig bleiende Hälfte unter diesen Zahlen sind lauter quadratische ichtreste.

Beispiel 1. Es sei

$$P=720=2^4.3^2.5,\ \text{also}\ S'''P=192,$$

ergiebt sich

$$\frac{1}{2^{\nu+1}}S'''P=\frac{192}{16}=12$$

nd es sind also unter den 192 Zahlen, welche kleiner als 720 und reıtive Primzahlen dazu sind, nur 12 quadratische Reste und die übrigen 80 sind quadratische Nichtreste. Um die sämmtlichen Reste zu erhalın, hat man das System der drei Bedingungscongruenzen

$$R^{2^{n-3}}=R^2\equiv 1\ (mod\ 16)$$
$$R^{\frac{1}{2}a^{\alpha-1}(a-1)}=R^3\equiv 1\ (mod\ 9)$$
$$R^{\frac{1}{2}b^{\beta-1}(b-1)}=R^2\equiv 1\ (mod\ 5)$$

ufzulösen mit der einen Vorsicht, dass man diejenigen 2 unter den 4 Vurzelwerthen von R, welche nicht quadratische Reste des Moduls 16 ind, ausscheidet. Die 4 bezeichneten Wurzeln sind:

$$1\ \ 7\ \ -7\ \ -1.$$

Offenbar ist 1 quadratischer Rest und ebenso —7; denn man hat

$$3^2 \equiv -7 \ (mod\ 16);$$

daraus folgt weiter nach dem Schlusstheoreme unter 5) im vorhergehenden Paragraphen, dass —1 und 7 Nichtreste, also auszuscheiden sind. Hiernach bekommt man:

$$R \equiv L \ (mod\ 16), \quad L = 1, -7;$$
$$R \equiv A \ (mod\ 9), \quad A = 1, 4, -2;$$
$$R \equiv B \ (mod\ 5), \quad B = 1, -1.$$

Nun bestimmt sich die Form aller Zahlen R, die nach den Moduln 16, 9, 5 die Reste L, A, B lassen, in bekannter Weise, wie folgt:

$$R \equiv 225L - 80A - 144B \ (mod\ 720).$$

Die 3 Glieder rechts geben, wenn man die Vielfachen von 720 abwirft:

$$225L = 225, -135$$
$$-80A = -80, -320, 160$$
$$-144B = -144, \ 144,$$

und man erhält daher folgende verschiedene Combinationen:

$$\begin{array}{llll} R \equiv 225-144-80, & 225+144-80, & -135-144-80, & -135+144-80; \\ \quad -320 & \quad -320 & \quad -320 & \quad -320 \\ \quad 160 & \quad 160 & \quad 160 & \quad 160 \end{array}$$

dieselben ergeben, wie es sein muss, 12 Zahlenwerthe für R, nämlich

$$\begin{array}{lrrrrl} R \equiv & 1 & 289 & -359 & -71 & (mod\ 720) \\ & -239 & 49 & 121 & -311 & \\ & 241 & -191 & -119 & 169 & \end{array}$$

Wir bemerken noch, dass wir dieselben Resultate auch durch Auflösung der Congruenz

$$R^{\frac{1}{2}\mu} = R^6 \equiv 1 \ (mod\ 720)$$

erhalten hätten. Nur hätten wir von deren 24 Wurzeln folgende 12 ausschliessen müssen:

$$\begin{array}{rrrr} -161 & 271 & -89 & 199 \\ 319 & 31 & -329 & -41 \\ 79 & -209 & 151 & -281. \end{array}$$

In der That muss, wenn R ein quadratischer Rest von P ist, ganz allgemein die Bedingungscongruenz

$$R^{\frac{1}{2}\mu} \equiv 1 \ (mod\ P)$$

bestehen, wo μ die im vorigen Paragraphen angegebene Bedeutung hat; aber es ist, ausser wenn P eine der beiden Formen p^n und $2p^n$ hat,

nicht umgekehrt durchaus nothwendig, dass jede Wurzel dieser Bedingungscongruenz auch ein quadratischer Rest sein müsse.

Beispiel 2. Es sollen die quadratischen Reste zu dem Modul $4P$ bestimmt werden, wenn P eine relative Primzahl zu 4 bezeichnet.

Der Modul 4 hat nur einen quadratischen Rest, nämlich 1 (nämlich 3 ist ein Nichtrest, weil die Congruenz $x^2 \equiv 3 \pmod 4$ für ganzzahlige x überhaupt nicht befriedigt werden kann); bezeichnet demgemäss R irgend einen zu P gehörigen quadratischen Rest und R' einen zu $4P$ gehörigen, so hat man, da 4 und P relative Primzahlen zu einander sind:

$$R' \equiv 1 \pmod 4,\ R' \equiv R \pmod P$$

und daher, indem man m' und m'' vermöge der Hülfscongruenzen

$$Pm' \equiv 1 \pmod 4,\ 4m'' \equiv 1 \pmod P$$

sich bestimmt, ist jeder Rest der gesuchten Art von der Form

$$R' \equiv Pm' + 4m''R.$$

Da die Grössen 4 und P nach der Voraussetzung keinen Theiler ausser 1 mit einander gemeinschaftlich haben, so muss P nothwendig eine ungerade Zahl sein und eine der beiden Formen

$$P = 4n+1,\ 4n-1$$

haben. Diesen Formen entsprechend findet man

$$m' = +1,\ -1$$
$$m'' = -n,\ +n$$

und es folgt

$$R' = P - 4nR,\ -P + 4nR.$$

Wir haben dem zu Folge das Theorem:

Die Zahlengrössen r mögen sämmtliche auf einen Modul von der Form $4n \pm 1$ bezüglichen quadratischen Reste bezeichnen: dann werden die auf einen Modul von der Form

$$P = 4(4n \pm 1)$$

bezogenen quadratischen Reste durch den Ausdruck

$$R = 1 \mp 4n(r-1)$$

repräsentirt. Die Anzahl der letzteren ist also, für beide Vorzeichen, gleich der Anzahl der ersteren.

Z. B. die quadratischen Reste von 105 sind nach der Tabelle unter Nr. 6) des vorigen §. folgende 6 Zahlen:

$$1 \quad 4 \quad 16 \quad 46 \quad -41 \quad -26;$$

da 105 von der Form $4.26+1$ ist, so sind mithin die quadratischen Reste von 420:

$$1-104.0 \quad 1-104.3 \quad 1-104.15$$
$$1-104.45 \quad 1+104.42 \quad 1+104.27$$

oder, wenn man die Rechnung ausführt und die Vielfachen von 420 weglässt:

$$1 \quad 109 \quad 121 \quad -59 \quad 169 \quad -131.$$

Um sich zu überzeugen, dass z. B. 109 wirklich ein quadratischer Rest ist, bemerke man, dass

$$109 \equiv 1 \ (mod\ 4)$$

und daher ist es quadratischer Rest von 4; ferner hat man

$$109 \equiv 4 = 2^2 \ (mod\ 105)$$

und es ist also auch quadratischer Rest von 105. Da nun die beiden Modul 4 und 105 relative Primzahlen zu einander sind, so ist es auch ein quadratischer Rest des Productes $4.105 = 420$.

Beispiel 3. Es sollen die quadratischen Reste des Moduls 36 bestimmt werden. Ihre Zahl ist nach der eben beendeten Erörterung die nämliche, wie bei dem Modul 9, also gleich $\frac{3.2}{2} = 3$. Um sie zu finden ist es in diesem Falle, wie überhaupt bei allen nicht sehr grossen Moduls, wohl am bequemsten sich die Reihe der relativen Primzahlen zu 36, die diese Grenze nicht überschreiten, zu bilden, nämlich:

$$\pm 1 \quad \pm 5 \quad \pm 7 \quad \pm 11 \quad \pm 13 \quad \pm 17,$$

dieselbe Glied für Glied zu quadriren und darauf die bezüglichen Reste durch directe Division mit dem Modul zu bestimmen. Gleich die 3 ersten Divisionen liefern die sämmtlichen quadratischen Reste, die nur möglich sind, nämlich:

$$1 \quad -11 \quad 13;$$

denn die nachfolgenden Divisionen erzeugen keine neuen von den früheren verschiedenen Reste, wie es auch sein muss, weil nicht mehr als 3 quadratische Reste existiren.

Beispiel 4. Es sei

$$P = 73, \ \tfrac{1}{2}S'''P = 36;$$

so sind 36 quadratische Reste vorhanden, welche identisch sind mit den Lösungen der Congruenz

$$R^{36} \equiv 1 \ (mod\ 73);$$

denn dass dieselbe Bestand habe, ist die ebensowohl nothwendige, als zureichende Bedingung dafür, dass die Congruenz $x^2 \equiv R \ (mod\ 73)$ möglich ausfalle. Die Lösungen der genannten Congruenz sind nun identisch mit der Gesammtmenge der Zahlen, welche entweder zu dem Exponenten 36 selbst, oder zu einem Theiler von 36 gehören, d. h. zu Folge der Tabelle in §. 11, wenn man nach der absoluten Grösse ordnet:

$$\pm 1 \ \pm 2 \ \pm 3 \ \pm 4 \ \pm 6 \ \pm 8$$
$$\pm 9 \ \pm 12 \ \pm 16 \ \pm 18 \ \pm 19 \ \pm 23$$
$$\pm 24 \ \pm 25 \ \pm 27 \ \pm 32 \ \pm 35 \ \pm 36.$$

Beispiel 5. Für

$$P = 2.5^2 = 50$$

findet man, indem man entweder die Congruenz

$$A^{\frac{1}{2}S'''50} = A^{10} \equiv 1 \ (mod\ 50)$$

sich auflöst, d. h. sich aus der Tabelle des p die Gesammtheit der zu den Exponenten

$$1 \quad 2 \quad 5 \quad 10$$

gehörigen Zahlen entnimmt, oder auch, indem man die Reihe der relativen Primzahlen zu 50, nämlich

$$\pm 1 \ \pm 3 \ \pm 7 \ \pm 9 \ \pm 11 \ \pm 13 \ \pm 17 \ \pm 19 \ \pm 21 \ \pm 23$$

quadrirt und darauf mit 50 dividirt, folgende 10 Reste

$$1 \quad 9 \quad -1 \quad -19 \quad 21 \quad 19 \quad -11 \quad 11 \quad -9 \quad -21$$

oder nach der absoluten Grösse geordnet:

$$\pm 1 \ \pm 9 \ \pm 11 \ \pm 19 \pm 21.$$

Die Reihe der Nichtreste zu 50 ist mithin;

$$\pm 3 \ \pm 7 \ \pm 13 \ \pm 17 \ \pm 23.$$

Beispiel 6. Die Zahl 46 soll darauf hin untersucht werden, ob sie ein quadratischer Rest von $105 = 3.5.7$ ist oder nicht. Es ist

$$46 \equiv 1,\ 1,\ 4 \ (mod\ 3,\ 5,\ 7);$$

nun ist 1 ein quadratischer Rest sowohl von 3, wie von 5, ebenso 4 ein quadratischer Rest von 7. Da nun die Modul 3, 5, 7 relative Primzahlen unter einander sind, so muss 46 auch ein quadratischer Rest des Productes 105 sein. In der That ergiebt die Betrachtung der Congruenz

$$x^2 \equiv 46 \ (mod\ 105)$$

oder auch ein Einblick in die auf den Modul 105 bezügliche Tabelle des vorigen §. sogleich, dass sie möglich ist und die acht Lösungen:

16 19 26 44 —44 —26 —19 —16

hat. Dies befindet sich in Uebereinstimmung damit, dass überhaupt 6 verschiedene quadratische Reste von 105 existiren und die 48 relativen Primzahlen zu 105, die kleiner als diese Zahl sind, sich nothwendig zu je 8 auf jeden Rest vertheilen müssen.

2) Betrachten wir jetzt den speciellen Fall, in welchem der Modul die Potenz irgend einer beliebigen ungeraden Primzahl ist, also von der Form

$$P = p^n, \text{ woher } S'''P = \pi = (p-1)p^{n-1};$$

so lässt sich dieser Fall immer auf die Betrachtung des einfacheren Falles zurückführen, in welchem der Modul die erste Potenz der nämlichen Primzahl p ist. Dies geschieht vermittelst des Theoremes: Jeder quadratische Rest des Moduls p ist auch ein quadratischer Rest des Moduls p^n und jeder quadratische Nichtrest des Moduls p ist auch ein quadratischer Nichtrest des Moduls p^n.

Nehmen wir Behuf des Beweises an, R sei ein quadratischer Rest des Moduls p, so ist nothwendig

$$R^{\frac{1}{2}(p-1)} \equiv 1 \ (mod\ p)$$

und es ist, wenn wir wieder mit den Doppelklammern den im vorigen Paragraphen angedeuteten Nebensinn verbinden, entweder

$$R^{\frac{1}{2}(p-1)} \equiv 1 \ ((mod\ p))$$

oder

$$R^{\frac{1}{2}(p-1)} \equiv 1 \ ((mod\ p^{\varrho})),\ \varrho \geqq 2;$$

daraus folgt zu Folge des nämlichen Paragraphen entweder

$$R^{\frac{1}{2}(p-1)p^{n-1}} \equiv 1 \ ((mod\ p^n))$$

oder

$$R^{\frac{1}{2}(p-1)p^{n-1}} \equiv 1 \ ((mod\ p^{\varrho+n-1})),$$

also, wie eine flüchtige Betrachtung der beiden Congruenzen zeigt, in beiden Fällen hat man

$$R^{\frac{1}{2}(p-1)p^{n-1}} \equiv 1 \ (mod\ p^n),$$

oder, mit anderen Worten, R ist ein quadratischer Rest des Moduls p^n; denn der Bestand der genannten Congruenz ist die nothwendige und zureichende Bedingung für die Möglichkeit der Congruenz $x^2 \equiv R \ (mod\ p^n)$.

Betrachten wir, indem wir die Zahl H die Reihe der Zahlen

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \ldots\ldots (p^{n-1}-1)$$

durchlaufen lassen, den Ausdruck

$$R' = R + Hp,$$

so bekommen wir p^{n-1} Zahlenwerthe für R', die alle nach dem Modul p einander congruent und quadratische Reste, dagegen nach dem Modul p^n zwar auch noch quadratische Reste, aber alle von einander verschieden sind. Mithin liefert jeder Rest R von p p^{n-1} einander congruente Reste von p^n und da es $\frac{1}{2}(p-1)$ von einander verschiedene R giebt, so bekommen wir in Gesammtheit $\frac{1}{2}(p-1)p^{n-1}$ Zahlen, welche alle von einander verschieden und quadratische Reste des Moduls p^n sind, in Uebereinstimmung mit dem Theoreme der vorhergehenden Nummer, nach welchem diese Anzahl gleichfalls herauskommen muss.

Beispiel. Es sei

$$p^2 = 13^2 = 169, \quad \pi = 156$$

und mithin die Zahl der quadratischen Reste gleich 78. Die quadratischen Reste von 13 werden leicht gefunden, indem man sich die Reihe der Zahlen < 13 und relative Primzahlen zu 13

$$\pm 1 \quad \pm 2 \quad \pm 3 \quad \pm 4 \quad \pm 5 \quad \pm 6$$

quadrirt und die zugehörigen Reste, nämlich:

$$1 \quad 4 \quad -4 \quad 3 \quad -1 \quad -3$$

oder, nach der absoluten Grösse geordnet:

$$1 \quad 3 \quad 4 \quad -4 \quad -3 \quad -1,$$

in Bezug auf den Modul 13 bestimmt. Indem man nun in die Formel

$$R + 13H$$

für R nach und nach alle diese Restwerthe und für H die Zahlen von 0 bis 12 substituirt, findet man die sämmtlichen quadratischen Reste von 169 in 6 Gruppen zu je 13 einander nach dem Modul 13 congruenten Zahlen vertheilt, wie folgt:

1	14	27	40	53	66	—90	—77	—64	—51	—38	—25	—12
3	16	29	42	55	68	—88	—75	—62	—49	—36	—23	—10
4	17	30	43	56	69	—87	—74	—61	—48	—35	—22	— 9
—4	9	22	35	48	61	74	—82	—69	—56	—43	—30	—17
—3	10	23	36	49	62	75	—81	—68	—55	—42	—29	—16
—1	12	25	38	51	64	77	—79	—66	—53	—40	—27	—14

Der Vollständigkeit halber wollen wir noch bemerken, dass man von den beiden Zahlenwerthen $\pm a$, deren Quadrat nach dem Modul p einen gegebenen speciellen Rest R giebt, zu denjenigen beiden Zahlenwerthen $\pm b$ aufsteigen kann, deren Quadrat nach dem Modul p^n denselben Rest giebt, vermittelst einer recurrirenden Beziehung zwischen beiden Systemen von Werthen aufsteigen kann.

Setzen wir nämlich die beiden Congruenzen

$$a^2 \equiv R \ (mod\ p^{m-1}),$$
$$b^2 \equiv R \ (mod\ p^m),$$

so muss, indem man die Möglichkeit beider voraussetzt, weil die letzte auch für den niedrigeren Modul p^{m-1} bestehen muss, b nothwendig von der Form

$$b = a + xp^{m-1}$$

sein; mithin ist

$$b^2 = a^2 + 2ap^{m-1}x + x^2p^{2m-2},$$

woher, durch Substitution von R für b^2,

$$R \equiv a^2 + 2ap^{m-1}x + x^2p^{2m-2} \ (mod\ p^m).$$

Nehmen wir nun m grösser als 1 an, so ist p^{2m-2} bestimmt ein Vielfaches des Moduls p^m und kann daher das Glied, in welchem es als ein Factor auftritt, ohne Weiteres weggeworfen werden. Dadurch resultirt die Congruenz

$$R \equiv a^2 + 2ap^{m-1}x \ (mod\ p^m),$$

die, weil nach der Voraussetzung die Differenz $R - a^2$ durch p^{m-1} theilbar sein muss, in die einfachere

$$\frac{R - a^2}{p^{m-1}} \equiv 2ax \ (mod\ p)$$

übergeht, welche in Bezug auf x vom ersten Grade und daher immer einen Werth, aber auch niemals mehr als diesen einen Werth für die Unbestimmte x liefert. Nachdem derselbe bestimmt ist, wird in der Congruenz

$$b \equiv a + xp^{m-1} \ (mod\ p^m)$$

die Relation ausgesprochen, vermöge deren aus dem gegebenen Zahlenwerthe a der entsprechende Zahlenwerth von b gefunden werden kann.

Indem man nach einander

$$m = 2 \ \ 3 \ \ 4 \ \ldots\ldots \ n-1$$

setzt, sieht man jetzt leicht ein, wie man von einem Zahlenwerthe a, der

dem Modul p entspricht, allmälig zu einem solchen Zahlenwerthe b aufsteigen kann, für welchen

$$b^2 \equiv R \ (mod\ p^n)$$

ist. Die Weise des Ueberganges erhellt näher aus nachfolgendem Schema:

$$a^2 \equiv R \ (mod\ p)$$

$$\frac{R-a^2}{p} \equiv 2ax \ (mod\ p) \quad a' \equiv a+px \ (mod\ p^2)$$

$$a'^2 \equiv R \ (mod\ p^2)$$

$$\frac{R-a'^2}{p^2} \equiv 2ax' \ (mod\ p) \quad a'' \equiv a'+p^2x' \ (mod\ p^3)$$

$$a''^2 \equiv R \ (mod\ p^3)$$

$$\frac{R-a''^2}{p^3} \equiv 2ax'' \ (mod\ p) \quad a''' \equiv a''+p^3x'' \ (mod\ p^4)$$

. . . .

. . . .

$$a^{(n-2)^2} \equiv R \ (mod\ p^{n-1})$$

$$\frac{R-a^{(n-2)^2}}{p^{n-1}} \equiv 2ax^{(n-2)} \ (mod\ p) \quad b \equiv a^{(n-2)}+p^{n-1}x^{(n-2)} \ (mod\ p^n)$$

Beispiel 1. Es sei

$$a=1 \quad p=3 \quad R=7$$

und es soll von der Congruenz $a^2 \equiv 1$ (mod 3) auf die Congruenz $b^2 \equiv 1$ (mod 81) übergegangen werden. Die Rechnung gestaltet sich wie folgt

$$1 \equiv 7 \ (mod\ 3), \ \frac{7-1}{3} = 2$$

$$2 \equiv 2x \ (mod\ 3), \quad x = 1, \quad a' \equiv 1+3=4 \ (mod\ 9)$$

$$16 \equiv 7 \ (mod\ 9), \ \frac{7-16}{9} = -1$$

$$-1 \equiv 2x' \ (mod\ 3), \quad x' = 1, \quad a'' \equiv 4+9 = 13 \ (mod\ 27)$$

$$169 \equiv 7 \ (mod\ 27), \ \frac{7-169}{27} = -6$$

$$-6 \equiv 2x'' \ (mod\ 3), \quad x''=0, \quad b \equiv 13 \ (mod\ 81).$$

Mithin entspricht dem Werth $a=1$ der Werth $b=13$ und ebenso würde man, wenn man es nicht schon im Voraus wüsste, finden können, dass sich die Werthe $a=-1$ und $b=-13$ gleichfalls entsprechen.

Beispiel 2. Die Zahl 20 ist ein quadratischer Rest des Moduls 11; denn man hat

$$20 \equiv 9 = (\pm 3)^2 \pmod{11};$$

man soll die beiden Zahlen finden, welche nach dem Modul

$$11^3 = 1331$$

demselben Reste 20 entsprechen.

$$p = 11, \; a = 3, \; R = 20$$

$$9 \equiv 20 \pmod{11}, \quad \frac{20-9}{11} = 1$$

$$1 \equiv 6x \pmod{11}, \qquad x = 2, \; a' \equiv 3+22 = 25 \pmod{121},$$

$$625 \equiv 20 \pmod{11}, \quad \frac{20-625}{121} = -5$$

$$-5 \equiv 6x' \pmod{11}, \qquad x' = 1, \; b \equiv 25+121 = 146 \pmod{1331}.$$

Hiernach ist $b = \pm 146$ und in der That besteht die Congruenz

$$(\pm 146)^2 = 21316 \equiv 20 \pmod{1331}.$$

3) Wir müssen dem Falle

$$P = 2^n, \; n \geqq 3$$

noch eine besondere Aufmerksamkeit zuwenden. So wie dieser Modul in seinem Verhalten überhaupt die grösste Aehnlichkeit mit einem aus mehreren Primfactoren zusammengesetzten Modul zeigt, so stimmt er auch in dieser Eigenschaft mit einem solchen überein, dass die Bedingungscongruenz

$$R^{\frac{1}{2}\pi} = R^{2^{n-3}} \equiv 1 \pmod{2^n}$$

wohl für jeden beliebigen quadratischen Rest erfüllt werden muss, aber durchaus noch keinen zureichenden Grund abgiebt, um auf die Eigenschaft einer Zahl quadratischer Rest des Moduls 2^n zu sein schliessen zu dürfen. Demgemäss wird es, wenn man die quadratischen Reste mit Zuziehung dieser Congruenz bestimmen will, darauf ankommen zu entscheiden, ob eine Wurzel quadratischer Rest oder Nichtrest ist. Hierbei leistet uns der Schlusssatz unter Nr. 5) des vorigen Paragraphen wesentliche Dienste. Derselbe lautet auf den betrachteten Fall übertragen folgendermassen:

a) **Je zwei zusammengehörige Wurzeln der Bedingungscongruenz**

$$R^{2^{n-3}} \equiv 1 \pmod{2^n},$$

die entweder die Form

$$+R, \; -R,$$

oder die Form

$$2^{\varkappa}h+1,\ 2^{\varkappa}h-1$$

haben, können nicht zu gleicher Zeit weder Reste noch Nichtreste der zweiten Potenz sein.

Wir erinnern daran, dass dem Exponenten $\varkappa$ in den genannten Formen die Werthe

$$\varkappa = n-1 \quad n-2 \quad n-3 \ \ldots\ldots\ 3$$

zukommen und der Grösse h die Werthe

$$h = 1 \quad 3 \quad 5 \quad 7 \quad 9 \ \ldots\ldots\ 2^{n-\varkappa}-1.$$

Unter dieser Voraussetzung bedeutet aber der Ausdruck

$$2^{\varkappa}h \pm 1$$

alle nur möglichen von einander verschiedenen Wurzeln unserer Bedingungscongruenz, mit Ausschluss der beiden Wurzeln $+1$, -1, welche übrigens auch vermittelst seiner erhalten werden, wenn man die Annahme $\varkappa = n$ zulassen will.

Sei nun R ein quadratischer Rest und von einer der beiden Formen

$$2^{\varkappa}h \pm 1,$$

so ist $-R$ von der Form

$$-2^{\varkappa}h \mp 1 \equiv 2^{\varkappa}(2^{n-\varkappa}-h) \mp 1 \ (mod\ 2^n)$$

und ein quadratischer Nichtrest. Hiernach ist aber wieder der Ausdruck

$$2^{\varkappa}(2^{n-\varkappa}-h) \pm 1 \equiv -2^{\varkappa}h \pm 1 \ (mod\ 2^n)$$

ein quadratischer Rest und es folgt mithin das Theorem:

b) Wenn irgend ein quadratischer Rest des Moduls 2 die Form

$$R \equiv 2^{\varkappa}h \pm 1 \ (mod\ 2^n)$$

hat, so existirt stets ein zweiter Rest von der Form

$$R' \equiv -2^{\varkappa}h \pm 1 \ (mod\ 2^n).$$

Vermittelst des Satzes unter *a*) ist es leicht einen dritten zu beweisen, der mit den beiden vorstehenden die Basis unserer Entwickelung bilden wird, nämlich: Wenn eine Zahl R quadratischer Rest irgend eines Moduls 2^n ist, so ist sie auch quadratischer Rest des Moduls 2^{n+1}.

Zu Folge der Voraussetzung ist R eine Wurzel der Congruenz

$$R^{2^{n-3}} \equiv 1 \ (mod\ 2^n)$$

und daher auch eine Wurzel der zweiten Congruenz

$$R^{2^{n-2}} \equiv 1 \ (mod\ 2^{n+1}).$$

In der That die Wurzeln der ersten sind von der Form

$$R = 2^{x}h \pm 1, \quad x = n-1 \quad n-2 \quad n-3 \; \ldots . \; 3,$$
$$h = 1 \;\; 3 \;\; 5 \;\; 7 \; \ldots\ldots \; 2^{n-x}-1,$$

die der zweiten dagegen von der Form

$$R' = 2^{x}h \pm 1, \quad x = n \quad n-1 \quad n-2 \; \ldots\ldots . \; 3$$
$$h = 1 \;\; 3 \;\; 5 \; \ldots . \; 2^{n-x}-1 \; \ldots .. \; 2^{n+1-x}-1$$

und aus der Vergleichung dieser beiden Formen erhellt unmittelbar die aufgestellte Behauptung. Demgemäss ist man berechtigt, in Anwendung des Satzes unter a), wenn man sich daselbst $n+1$ statt n gesetzt denkt, zu schliessen, dass, wenn die eine der Formen

$$2^{x}h+1, \; 2^{x}h-1$$

ein quadratischer Nichtrest ist, die andere ein Rest des Moduls 2^{n+2} ist. Wenn also irgend ein specielles

$$R = 2^{x}h \pm 1$$

ein quadratischer Rest von 2^{n} und zugleich ein Nichtrest von 2^{n+1} sein könnte, so müsste der Ausdruck

$$2^{x}h \mp 1$$

nothwendig ein Rest des Moduls 2^{n+1} und darum auch des niedrigeren Moduls 2^{n} sein, d. h. jeder der beiden Ausdrücke $2^{x}h+1$ und $2^{x}h-1$ wäre ein Rest von 2^{n}, der eine nach der Voraussetzung und der andere nach der Annahme. Da dies unstatthaft ist, so muss der ausgesprochene Satz Geltung haben.

Unser nächstes Ziel muss sein zu unterscheiden, welche der beiden Formen

$$2^{x}h \pm 1,$$

deren die Wurzeln unserer Bedingungscongruenz fähig sind, in jedem speciellen Falle ein quadratischer Rest sei. Bilden wir uns, um etwas durch Induction zu erfahren, die Quadrate der ungeraden Zahlen

$$\pm 1 \;\; \pm 3 \;\; \pm 5 \;\; \pm 7 \; \ldots .$$

und dividiren dieselben nach der Reihe durch die Modul

$$8 \;\; 16 \;\; 32,$$

so zeigen die respectiven Reste, wenn man blos positive zulässt, überall die dem oberen Vorzeichen entsprechende Form. Um also darzuthun, dass die Form

$$2^{x}h+1$$

allgemein gültig sei, haben wir nur nöthig nachzuweisen, dass, wenn die Reste von 2^n diese Form haben, dieselbe Form auch den Resten von 2^{n+1} zukommen.

Die quadratischen Reste des Moduls 2^n werden mit Ausschluss des Restes 1 dargestellt durch die (2^{n-x-1})gliedrige Reihe

$$2^x.1+1 \quad 2^x.3+1 \quad 2^x.5+1 \; \ldots\ldots\ldots\ldots \; 2^x(2^{n-x}-1)+1,$$

in der dem Exponenten x die oben angegebenen Werthe zukommen. Nun sind dieselben nach *c*) zu gleicher Zeit Reste des Moduls 2^{n+1}; dies angenommen folgt nach *b*) eine zweite Reihe von Resten desselben Moduls 2^{n+1}, nämlich:

$$-2^x.1+1 \quad -2^x.3+1 \quad -2^x.5+1 \; \ldots\ldots\ldots \; -2^x(2^{n-x}-1)+1.$$

Man kann nun leicht zweierlei darthun, zuerst dass die Reste beider Reihen nach dem Modul 2^{n+1} von einander verschieden sind, und dann dass sie sämmtlich unter der angegebenen Form stehen. Sie sind zuerst verschieden. Denn wäre

$$2^x h+1 \equiv -2^x h'+1 \; (mod\; 2^{n+1}),$$

so würde folgen, indem man die Grösse 1 beiderseits weglässt und dann mit 2^x dividirt,

$$h+h' \equiv 0 \; (mod\; 2^{n+1-x}),$$

was nicht angeht, da h und h' beide ungerade Zahlen unter 2^{n-x} sind. — Die Reste der ersten Reihe ferner haben unmittelbar alle die Form $2^x h+1$ und die Reste der zweiten Reihe erhalten alle dieselbe Form, wenn man überall den Modul 2^{n+1} hinzuaddirt; denn man bekommt dann als allgemeines Glied

$$2^x(2^{n+1-x}-h)+1$$

und darin ist h immer kleiner als 2^{n-x}, mithin die Grösse in der Klammer irgend einer zwischen den Grenzen 2^{n+1-x} und 2^{n-x} befindlichen ungeraden Zahl gleich.

Sehen wir nun zu, wie viele quadratische Reste wir in unsere Betrachtung gezogen haben, so ist klar, dass jede auf ein specielles x bezügliche Doppelreihe

$$2.2^{n-x-1} = 2^{n-x}$$

Reste umfasst. Da nun x die Werthe

$$n-1 \quad n-2 \quad n-3 \; \ldots\ldots \; 3$$

haben kann, so erhalten wir in Gesammtheit

$$2+2^2+2^3+\ldots.+2^{n-3}=2^{n-2}-2$$

quadratische Reste von 2^{n+1}. Die Vollzahl ist aber für diesen Modul 2^{n-2}, also fehlen noch 2. Der eine entspricht dem Werthe

$$x=n$$

und hat die Form

$$-2^n+1 \equiv 2^n+1 \ (mod\ 2^{n+1}).$$

Zunächst nämlich erkennt man leicht, dass diese Form eine Wurzel der auf den Modul 2^{n+1} bezogenen Bedingungscongruenz ist, für welche x den bezeichneten Werth annimmt: sie kann also quadratischer Rest sein; dass sie es wirklich ist, folgt daraus, dass die Congruenz

$$x^2 \equiv 2^n+1 \ (mod\ 2^{n+1})$$

durch die Annahme

$$x \equiv 2^{n-1}-1 \ (mod\ 2^{n+1})$$

befriedigt wird, wofern n grösser als 3 gegeben ist.

Der letzte quadratische Rest endlich, der noch fehlt und, wenn man will, auf den Werth

$$x=n+1$$

des Index x bezogen werden kann, ist 1, welches sich gleichfalls der Form $2^x h+1$ unterordnet. Hiermit ist dargethan, dass alle Reste von 2^{n+1} ohne Ausnahme diese Form haben und unsere obige Vermuthung mithin bewiesen.

Aus dem Gange des Beweises erhellt, dass man die quadratischen Reste des Moduls 2^{n+1} in $n-1$ verschiedene Klassen eintheilen kann, je nach den verschiedenen Werthen des x, durch welche sie erzeugt werden. Die erste Klasse entspricht dem Werthe $x=n+1$ und besteht aus der einzigen Zahl 1; die zweite Klasse entspricht dem Werthe $x=n$ und enthält gleichfalls nur einen einzigen Rest, nämlich:

$$-2^n+1.$$

Die folgenden $n-3$ Klassen endlich beziehen sich auf die Werthe

$$x=n-1 \quad n-2 \quad n-3 \ \ldots.. \ 3$$

und setzen sich immer aus einer geraden Anzahl von Resten zusammen, derartig, dass jede auf ein specielles x bezügliche Restklasse sich aus 2 Partien von in den kleinsten Zahlen ausgedrückten Resten zusammensetzt. Die eine Partie enthält lauter positive Zahlen, die eine um 2^x fortschreitende arithmetische Progression bilden, die zweite Partie lauter negative Zahlen, die eine ähnliche Progression bilden und deren absolute Zahlen-

werthe um 2 kleiner sind, als die Zahlen der ersten Partie. In der That gestatten, wie wir gesehen haben, die quadratischen Reste von 2^{n+1} folgende Anordnung:

$$\begin{array}{ll} 2^{\varkappa}.1+1 & -2^{\varkappa}.1+1 \\ 2^{\varkappa}.3+1 & -2^{\varkappa}.3+1 \\ 2^{\varkappa}.5+1 & -2^{\varkappa}.5+1 \\ \ldots\ldots & \ldots\ldots \\ \ldots\ldots & \ldots\ldots \\ 2^{\varkappa}(2^{n-\varkappa}-1)+1 & -2^{\varkappa}(2^{n-\varkappa}-1)+1 \end{array}$$

und man ist daher folgendes Theorem auszusprechen berechtigt:

Die quadratischen Reste des Moduls 2^{n+1} sind bis auf die beiden Reste

$$1, \ -2^{n}+1$$

inbegriffen in der Formel

$$\pm 2^{\varkappa}h+1,$$

in der den Grössen $\varkappa$ und h die Zahlenwerthe

$$\begin{array}{l} \varkappa = n-1 \quad n-2 \quad n-3 \;\ldots\ldots\; 3 \\ h = 1 \quad 3 \quad 5 \quad 7 \;\ldots\ldots\; 2^{n-\varkappa}-1 \end{array}$$

zukommen.

Es wird nicht überflüssig sein zur Veranschaulichung der gewonnenen Resultate folgende Tabelle für die Modul 8, 16, 32, 64, 128, 256 beizufügen:

$n-\varkappa=$	1	2	3	4	5	6
$\varkappa=$	$n+1$	n	$n-1$	$n-2$	$n-3$	$n-4$
$2^{2+1}=8$	1					
$2^{3+1}=16$	1	−7				
$2^{4+1}=32$	1	−15	9 −7			
$2^{5+1}=64$	1	−31	17 −15	9 25 −7 −23		
$2^{6+1}=128$	1	−63	33 −31	17 49 −15 −47	9 25 41 57 −7 −23 −39 −55	
$2^{7+1}=256$	1	−127	65 −63	33 97 −81 −95	17 49 81 113 −15 −47 −79 −111	9 25 41 57 73 89 105 121 −7 −23 −39 −55 −71 −87 −103 −119

Der Index $n-\varkappa$ bezeichnet hierbei die Klasse, unter welche der vertikal darunter befindliche quadratische Rest gehört und der Index $\varkappa$ den Exponenten von 2 in der Formel

$$\pm 2^{\varkappa}h+1,$$

welche alle Reste der betrachteten Klasse umfasst. So z. B. sind die

Reste der dritten Klasse nach dem Modul 32 gleich 9 und —7 und das betreffende $x = n - 1 = 4 - 1 = 3$ und damit in Uebeinstimmung ist:

$$9 = 2^3.1+1, \quad -7 = -2^3.1+1.$$

Ferner sind die Reste der 4ten Klasse zu dem Modul $2^{6+1} = 128$:

$$17 \quad 49 \quad -15 \quad -47,$$

und das betreffende x ist $n - 2 = 6 - 2 = 4$. In der That hat man

$$17 = 2^4.1+1, \quad 49 = 2^4.3+1,$$
$$-15 = -2^4.1+1, \quad -47 = -2^4.3+1.$$

4) In allen vorhergehenden Erörterungen ist die 0 als quadratischer Rest ausdrücklich nicht in Betracht gezogen worden. Wenn man nun von dem Modul p (mag derselbe eine gerade oder ungerade Primzahl sein) zu dem Modul p^n übergeht, so macht sich die besondere Betrachtung der Zahlen

$$0 \quad p \quad 2p \quad 3p \; \ldots\ldots \; p^n - p$$

nothwendig, welche nach dem Modul p alle der 0 congruent, dagegen nach dem Modul p^n einander incongruent sind. Nehmen wir zunächst eine beliebige Zahl von der Form Ap, wo A eine relative Primzahl zu p ist, heraus, so kann die Congruenz

$$x^2 \equiv Ap \; (mod \; p^n)$$

keinesfalls bestehen, weder für ein x, welches relative Primzahl zu p ist, noch für ein x, welches den Factor p enthält: denn im letzteren Falle wäre die linke Seite der Congruenz mindestens durch p^2 ohne Rest theilbar, also müsste es auch die rechte Seite Ap sein, im Widerspruche zu der Voraussetzung, dass A kein Vielfaches von p ist; der erstere Fall ist selbstverständlich unstatthaft.

Demgemäss nach Ausscheidung der bezeichneten Vielfachen, die auf jeden Fall sämmtlich Nichtreste sind, bleibt noch die Reihe der Zahlen

$$0 \quad p \quad p^2 \quad p^3 \; \ldots\ldots \; p^{n-1}$$

zu discutiren. Nehmen wir zuerst eine ungerade Potenz von p, so haben wir im Allgemeinen die Möglichkeit der Congruenz

$$x^2 \equiv p^{2x+1} \; (mod \; p^n)$$

zu untersuchen. Diese Möglichkeit vorausgesetzt müsste x nothwendig durch irgend eine Potenz von p theilbar sein, also x^2 eine gerade Potenz von p als Factor enthalten, d.h. indem x eine relative Primzahl zu p bezeichnet, von der Form $X^2 p^{2\lambda}$ sein; mithin folgte:

$$X^2 p^{2\lambda} \equiv p^{2x+1} \pmod{p^n},$$

eine in jedem Falle unstatthafte Congruenz, mag nun 2λ grösser oder kleiner als $2x+1$ sein. Im ersten Falle würde man nämlich aus ihr erhalten

$$X^2 p^{2\lambda-2x-1} \equiv 1 \pmod{p^{n-(2x+1)}}$$

also, da $p^{n-2x-1} \geqq 1$ ist,

$$X^2 p^{2\lambda-2x-1} \equiv 1 \pmod{p},$$

was nicht angeht, da die linke Seite offenbar ein Vielfaches von p ist. Im zweiten Falle dagegen würde man

$$X^2 \equiv p^{2x+1-2\lambda} \pmod{p^{n-2\lambda}}$$

erhalten, welches gleichfalls ein Widerspruch ist, da die linke Seite eine mit p incongruente, dagegen die rechte Seite eine mit p congruente Zahl ist.

Also kann die obige Congruenz überhaupt für kein reelles x bestehen, d. h. jede ungerade Potenz von p ist ein quadratischer Nichtrest des Moduls p^n.

Betrachten wir endlich irgend eine gerade Potenz p^{2x}, so ist klar, dass dieselbe ein quadratischer Rest ist: denn der Congruenz

$$x^2 \equiv p^{2x} \pmod{p^n},\ 2x < n$$

geschieht Genüge durch die beiden reellen Werthe $x = \pm p^x$.

Wenn P ein beliebig zusammengesetzter Modul von der Form

$$P = a^\alpha\ b^\beta\ c^\gamma\ \ldots.$$

ist, so sind, indem man unter a^α, b^β, c^γ, ... diejenigen geraden Potenzen von den Grössen a, b, c, ... versteht, welche zunächst unter P liegen, die Zahlen der Reihen

$$\begin{array}{cccccc} 0 & a^2 & a^4 & a^6 & \ldots. & a^{\alpha'}, \\ 0 & b^2 & b^4 & b^6 & \ldots. & b^{\beta'}, \\ 0 & c^2 & c^4 & c^6 & \ldots. & c^{\gamma'}, \\ & & \ldots\ldots & & & \\ & & \ldots\ldots & & & \end{array}$$

sämmtlich quadratische Reste von P und ausser ihnen noch alle diejenigen Producte aus 2 oder mehreren dieser Zahlen, welche kleiner als P sind. Sei z. B. der Modul $P = 720$, so findet man folgende aus einfachen Potenzen bestehende Restreihen:

4 16 64 256
9 81
25 625

und folgende, die aus zusammengesetzten Potenzen besteht:

0 36 324 100 144 400 576.

Es kommen also zu den früher gefundenen 12 quadratischen Resten, welche relative Primzahlen zu 720 sind, noch 15 neue hinzu, welche mit 720 irgend einen Factor gemeinschaftlich haben.

4) Fassen wir die vorstehenden Entwickelungen zusammen, so erhellt, dass alle nur möglichen Fälle, in denen der Modul eine irgend wie zusammengesetzte Zahl ist, sich auf zwei Fundamentalfälle zurückführen lassen. Der eine tritt ein, wenn eine beliebige Potenz von 2 als Modul gegeben ist, und derselbe ist bereits in erschöpfender Weise abgehandelt. In dem anderen allgemeineren Falle ist der Modul eine beliebige ungerade Primzahl und unter dieser speciellen Annahme werden wir daher von jetzt ab die weitere Betrachtung fortführen.

Als in dem, was vorhergeht, mit enthalten können wir sogleich folgende wesentliche Theoreme aufstellen:

a) Eine Zahl *a* ist, wenn die Congruenz

$$a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$$

besteht, ein quadratischer Rest des Moduls p, dagegen, wenn die Congruenz

$$a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$$

besteht, ein quadratischer Nichtrest desselben Moduls.

Die Reihe der Zahlen

$$1 \ 2 \ 3 \ 4 \ \ldots\ldots \ p-2 \ p-1$$

oder, wenn man die kleinsten Reste vorzieht,

$$\frac{p-1}{2} \ \ldots\ldots \ 3 \ 2 \ 1 \ -1 \ -2 \ -3 \ \ldots\ldots \ -\frac{p-1}{2}$$

enthält $\frac{p-1}{2}$ von einander verschiedene quadratische Reste und alle übrigen quadratischen Reste, die keine Vielfachen von p und grösser als p sind, müssen irgend einem der vorhergehenden Reste congruent sein; die übrig bleibenden Zahlen der Reihe, deren

Anzahl gleichfalls $\frac{p-1}{2}$ ist, sind sämmtlich quadratische Nichtreste und zwar alle nur möglichen, die von einander verschieden sind.

Der Kürze halber wollen wir mit Legendre den Rest, welchen die Potenz $a^{\frac{p-1}{2}}$ nach dem Modul p lässt, mit $\left(\frac{a}{p}\right)$ bezeichnen, so dass man

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (mod\ p)$$

hat; dann kann man den ersten unter den beiden vorhergehenden Sätzen wie folgt aussprechen:

b) Eine Zahl a ist quadratischer Rest oder Nichtrest des Moduls p, je nachdem man $\left(\frac{a}{p}\right) = +1$ oder $= -1$ hat.

Ferner kann man mit leichter Mühe die Gleichung

$$\left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right) = \left(\frac{aa'}{p}\right)$$

herleiten; denn es ist

$$a^{\frac{p-1}{2}} \cdot a'^{\frac{p-1}{2}} = (aa')^{\frac{p-1}{2}} \equiv \left(\frac{aa'}{p}\right)$$

und daraus geht der Satz hervor:

c) Sind zwei Zahlen a und a' zu gleicher Zeit entweder quadratische Reste oder quadratische Nichtreste, so ist das Product stets ein quadratischer Rest zu p: ist dagegen die eine dieser Zahlen ein quadratischer Rest, die andere ein quadratischer Nichtrest, so ist das Product aa' stets ein quadratischer Nichtrest. (Beide Zahlen a und a' werden hierbei in Uebereinstimmung mit unserer obigen Annahme als von 0 verschieden vorausgesetzt.)

Beispiel. Die Zahl 32 soll untersucht werden, ob sie ein quadratischer Rest von dem Modul 73 ist. Indem man sich die Quadrate der 9 ersten aufeinander folgenden Zahlen bildet, findet man ohne Weiteres, dass die Zahlen

$$4 = 2^2,\ 8 = 9^2 - 73$$

quadratische Reste von 73 sind, mithin ist es auch $32 = 4 \cdot 8$. In der That findet sich durch weiteres Versuchen

$$18^2 \equiv 32\ (mod\ 73).$$

Ferner ist 7 ein quadratischer Nichtrest von 73; mithin kann 49 als ein

Product zweier Nichtreste gelten und muss daher Rest sein. In der That ist es dies; denn der Congruenz

$$x^2 \equiv 49 \ (mod \ 73)$$

geschieht durch den Zahlenwerth $x = 7$ Genüge. Dagegen muss $4.7 = 28$ ein Nichtrest sein und das bestätigt sich auch; denn die Reihe sämmtlicher Reste besteht aus den Zahlen

1	2	3	4	6	8	9	12	16
18	19	23	24	25	27	32	35	36
—36	—35	—32	—27	—25	—24	—23	—19	—18
—16	—12	— 9	— 8	— 6	— 4	— 3	— 2	— 1.

In weiterer Verallgemeinerung des letzten Satzes ergiebt sich, *dass eine Zahl, die ein Product von lauter Resten ist, nothwendig ein quadratischer Rest sein müsse; dagegen wenn ein Theil der Factoren aus Nichtresten besteht, so ist sie ein Rest, wenn dieselben in gerader Anzahl und ein Nichtrest, wenn dieselben in ungerader Anzahl vorhanden sind.* Hiernach ist z. B, $125 = 5.5.5$ ein Nichtrest von 73; wirklich ist $125 = 146 - 19$ und -19 nicht unter den Resten.

Auf diese Weise wird die Reihe der Zahlen von 1 bis $p-1$, welche untersucht werden müssen, bedeutend reducirt, nämlich alle zusammengesetzten Zahlen fallen aus und es bleibt blos die Reihe der Primzahlen übrig. Es giebt aber auch noch einige andere Umstände, welche zur Verminderung der Zahl der zu untersuchenden Zahlen beitragen. Wenn man nämlich irgend eine Primzahl durch 4 dividirt, so kann entweder 1 oder 3 als Rest bleiben und es geht hieraus hervor, dass jede Primzahl eine der beiden Formen

$$4n+1, \ 4n+3 \text{ oder } 4n-1$$

haben muss und man kann also die Primzahlen in Bezug auf 4 in 2 Klassen eintheilen, je nachdem sie von der einen oder der andern der genannten Formen sind. Nehmen wir zuerst an, dass p von der Form $4n+1$ und a ein quadratischer Rest des Moduls p sei, so ist

$$\frac{p-1}{2} = 2n$$

und die Bedingungscongruenz

$$a^{2n} \equiv 1 \ (mod \ p)$$

muss bestehen. Dieser Gleichung genügt aber ebensowohl $+a$ wie $-a$; mithin wird die ebensowohl erforderliche wie ausreichende Bedingung dafür, dass $-a$ ein quadratischer Rest sei, erfüllt. Jeder Rest $+a$ liefert demgemäss sofort einen zweiten, nämlich $-a$.

Ist dagegen p von der Form $4n-1$ und a gleichfalls ein quadratischer Rest von p, so wird die Bedingungscongruenz

$$a^{\frac{p-1}{2}} = a^{2n-1} \equiv 1 \pmod{p}$$

nur für $+a$, aber nicht für $-a$ erfüllt; vielmehr ist

$$(-a)^{2n-1} \equiv -1 \pmod{p},$$

d. h. die Zahl $-a$ ist ein quadratischer Nichtrest.

Hiernach kann man folgendes Theorem aussprechen:

d) Wenn p eine Primzahl von der Form $4n+1$ ist und irgend eine Zahl a ein quadratischer Rest von p ist, so ist auch $-a$ oder, was dasselbe ist, $p-a$ ein quadratischer Rest von p. Hat dagegen die Primzahl p die Form $(4n+3$ oder $(4n-1$ und ist a ein quadratischer Rest von p, so ist $-a$ (oder $p-a$) ein quadratischer Nichtrest von p.

Wie man augenblicklich einsieht, ist aber trotz aller dieser Sätze, welche allerdings die Aufsuchung der quadratischen Reste für einen gegebenen Modul p erleichtern, dies Geschäft noch immer ungemein langwierig, derartig, dass es sich nicht wohl ohne Hülfstafeln ausführen lässt. Ist man im Besitz von Tabellen für die Congruenz

$$x^q \equiv 1 \pmod{p},$$

wo q irgend einen Theiler von $p-1$ bezeichnet, so bilden ganz einfach die Zahlen, welche zu dem Exponenten $\frac{p-1}{2}$ oder einem Theiler desselben gehören, die Gesammtheit der möglichen von einander verschiedenen quadratischen Reste (immer die 0 nicht mitgerechnet); denn alle diese Zahlen befriedigen die Bedingungscongruenz

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

und stellen zugleich alle nur möglichen Lösungen derselben dar, wie sich nach einem in der Einleitung enthaltenen, das S''' betreffenden Satze leicht nachweisen lässt. Mithin werden dieselben Methoden, welche zur

Berechnung der genannten Zahlen dienen, auch zur Berechnung der quadratischen Reste verwandt werden können und es ergiebt sich noch beiläufig der Satz, dass alle primitiven Wurzeln des Moduls p quadratische Nichtreste sind.

Unter solchen Umständen hat man das Problem umgekehrt und untersucht, in welchen Fällen eine gegebene Primzahl a ein quadratischer Rest oder Nichtrest für eine gegebene Primzahl p sei oder von welcher Form die Primzahl p sein müsse, damit eine gegebene Zahl a ein quadratischer Rest oder Nichtrest derselben sei. Die Lösung dieses Problems beruht auf dem berühmten Reciprocitätsgesetze, welches in seiner Allgemeinheit von Legendre herrührt und welches man jetzt für das schönste in der höheren Arithmetik hält. Es beschäftigten sich damit nach einander die berühmtesten Analytiker bis in die neueste Zeit hinein, nämlich Euler, Lagrange, Legendre und Gauss, welcher 6 Beweise dafür gegeben hat. Wir wollen, ehe wir dazu übergehen, nach dem Vorgange des letzteren erst eine Anzahl specieller Fälle erörtern, vermöge deren die Erfinder durch Induction zu dem allgemeinen Satze gelangt sind, und um hierbei ein bequemes Material für die bei diesen Erörterungen vorkommenden Inductionen zu bieten, wollen wir die folgende Zusammenstellung von quadratischen Resten für die ersten Primzahlen geben, in welcher indessen von 43 ab nur Primzahlen aufgenommen sind.

p	
3	1
5	1 —1
7	1 2 —3
11	1 3 4 5 —2
13	1 3 4 —4 —3 —1
17	1 2 4 8 —8 —4 —2 —1
19	1 4 5 6 7 9 —8 —3 —2
23	1 2 3 4 6 8 9 —11 —10 —7 —5
29	1 4 5 6 7 9 13 —13 —9 —7 —6 —5 —4 —1
31	1 2 4 5 7 8 9 10 14 —15 —13 —12 —11 —6 —3
37	1 3 4 7 9 10 11 12 16 —16 —12 —11 —10 —9 —7 —4 —3 —1
41	1 2 4 5 8 9 10 16 18 20 —20 —18 —16 —10 —9 —8 —5 —4 —2 —1

p	
43	1 4 6 9 10 11 13 14 15 16 17 21 —20 —19 —18 —12 —8 —7 —5 —3 —2
47	1 2 3 7 17 —23 —19 —13 —11 —5
53	1 7 11 13 17 —17 —13 —11 —7 —1
59	1 3 5 7 17 19 29 —23 —13 —11 —2
61	1 3 5 13 19 —19 —13 —5 —3 —1
67	1 17 19 23 29 —31 —13 —11 —7 —5 —3 —2
71	1 2 3 5 19 29 —31 —23 —17 —13 —11 —7
73	1 2 3 19 23 —23 —19 —3 —2 —1
79	1 2 5 11 13 19 23 31 —37 —29 —17 —7 —3
83	1 3 7 11 17 23 29 31 37 41 —19 —13 —5 —2
89	1 2 5 11 17 —17 —11 —5 —2 —1
97	1 2 3 11 31 43 47 —47 —43 —31 —11 —3 —2 —1
101	1 5 13 17 19 23 31 37 43 47 —47 —43 —37 —31 —23 —19 —17 —13 —5 —1

§. 16.

Betrachtung specieller quadratischer Reste.

1) Wir werden weiter unten öfters solchen Zahlenpaaren, wie a und b, begegnen, deren Product nach einem gegebenen Modul p den gleichfalls unveränderlichen Rest r lässt, so dass die Congruenz

$$ab \equiv r \ (mod\ p)$$

erfüllt wird. Wir wollen solche Zahlen einander nach dem Modul p für die Zahlengrösse r conjugirt nennen und betrachten natürlich hierbei nur solche Zahlen a und b, welche kleiner als die ungerade Primzahl p sind. Dieses vorausgesetzt erhellt unmittelbar aus der Thatsache, dass die genannte Congruenz in Bezug auf b vom ersten Grade ist, der Satz, dass zu jeder beliebigen Zahl stets eine und nur eine conjugirte Zahl existirt. Im Allgemeinen werden je zwei conjugirte Zahlen von einander verschieden sein müssen; wenn sie in eine zusammenfallen, d. h. wenn eine Zahl sich selber conjugirt sein soll, so muss dieselbe nothwendig eine Lösung der Congruenz

$$x^2 \equiv r \ (mod\ p)$$

sein und da dieselbe, gemäss unserer über die Natur des Moduls p gemachten Voraussetzung, wenn sie überhaupt möglich ist, 2 Wurzeln und sonst weiter keine hat, so folgt das Theorem:

Wenn r ein quadratischer Nichtrest ist, so giebt es keine Zahl, die sich selbst conjugirt sein könnte, und die Zahlen aller Paare sind von einander verschieden; wenn dagegen r ein quadratischer Rest ist, so existiren immer 2 Zahlen, welche sich selber conjugirt sind, die übrig bleibenden Zahlen bilden lauter Paare mit verschiedenen Zahlen. Die Anzahl der Paare ist im ersten Falle $\frac{p-1}{2}$, im zweiten $\frac{p+1}{2}$.

Wenn r gleich 1 ist, so wollen wir a und b schlechthin conjugirte Zahlen nennen. In diesem Falle sind die beiden sich selbst conjugirten Zahlen offenbar 1 und -1 oder $p-1$ und es folgt das specielle Theorem:

Von den zwischen 1 und $p-1$ befindlichen Zahlen ist keine, die sich selbst (für den Rest 1) conjugirt sein könnte.

Aus dieser Theorie fliesst mit der grössten Leichtigkeit der Wilson'sche Satz. Nämlich zu Folge des letzten Satzes lassen sich die Zahlen

$$2\ 3\ 4 \ldots\ldots p-2,$$

deren Anzahl $p-3$ ist, in $\frac{p-3}{2}$ Gruppen zu je zwei eintheilen, deren Product 1 ist, also folgt durch Multiplication

$$2.3.4 \ldots. (p-2) \equiv 1 \ (mod.\ p)$$

und multiplicirt man diese Congruenz mit der nachfolgenden

$$1.(p-1) \equiv -1,$$

so erhält man

$$1.2.3.4 \ldots. (p-2)(p-1) \equiv -1 \ (mod\ p).$$

Bildet man sich das Product aus den nämlichen Zahlen von 1 bis $p-1$, indem man sie sich in Gruppen zu je zwei, die einander für den Rest r conjugirt sind, zerlegt denkt, so erhält man, wenn r ein quadratischer Nichtrest ist,

$$1.2.3 \ldots. (p-1) \equiv r^{\frac{p-1}{2}},$$

mithin durch Anwendung des Satzes von Wilson

$$r^{\frac{p-1}{2}} \equiv -1 \ (mod\ p),$$

d. h. die bekannte Bedingungscongruenz, welche für jeden quadratischen Nichtrest stattfindet.

Ist dagegen r ein quadratischer Rest, so folgt, wenn a und b die beiden sich selbst conjugirten Zahlen bezeichnen:

$$1.2.3 \ldots (p-1).ab \equiv r^{\frac{p+1}{2}} \pmod{p},$$

woher abermals nach dem Satze von Wilson:

$$ab \equiv -r^{\frac{p+1}{2}} \equiv -r.r^{\frac{p-1}{2}} \pmod{p}.$$

Nun hat man aber, da a und b sich selber conjugirt sind,

$$a^2 \equiv r, \quad b^2 \equiv r \pmod{p},$$

also durch Multiplication

$$a^2b^2 \equiv r^2 \pmod{p}$$

und damit diese Congruenz bestehen könne, muss entweder

$$ab \equiv +r \pmod{p}$$

oder

$$ab \equiv -r \pmod{p}$$

sein. Ersteres ist nicht statthaft; denn es würde daraus

$$a^2 \equiv ab, \quad a \equiv b$$

hervorgehen, im Widerspruche damit, dass offenbar

$$b \equiv -a$$

ist. Also bleibt nur die zweite Annahme

$$ab \equiv -r \pmod{p}$$

möglich und es wird durch Einsetzung dieses Werthes in die vorhergehende Congruenz für ab

$$-r \equiv -r.r^{\frac{p-1}{2}},$$

d. h. es besteht die Bedingungscongruenz

$$r^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

welche, wie wir wissen, ausdrückt, dass r ein quadratischer Rest ist.

Diese Andeutungen mögen genügen, um den Schluss ziehen zu lassen, dass man die bisherige Theorie der quadratischen Reste auch auf die Betrachtung der conjugirten Zahlen hätte basiren können.

Beispiele. Indem wir die Zahl 17 als Modul annehmen, wollen wir die Paare conjugirter Zahlen, welche für die Reste 1 und 3 erhalten werden, ohne Weiteres folgen lassen und schicken nur die Bemerkung

vorher, dass, sobald die verschiedenen auf den Rest 1 bezüglichen Gruppen berechnet sind, die irgend einem anderen Reste r entsprechenden Gruppen sich leicht daraus ableiten lassen. Denn seien a und b zwei Zahlen, welche der Congruenz

$$ab \equiv 1 \ (mod\ p)$$

Genüge leisten, so wird offenbar die Congruenz

$$a'b' \equiv r \ (mod\ p)$$

befriedigt, sowohl durch die Annahmen

$$a' \equiv a,\ b' \equiv ar,$$

wie auch durch die Annahmen

$$a' \equiv ar,\ b' \equiv b.$$

$p = 17$	$r = 1$	$p = 17$	$r = 3$
1	1	1	3
2	$9 \equiv -8$	2	$10 \equiv -7$
3	6	4	5
4	$13 \equiv -4$	7	$15 \equiv -2$
5	7	8	$11 \equiv -6$
8	$15 \equiv -2$	$9 \equiv -8$	6
$10 \equiv -7$	$12 \equiv -5$	$12 \equiv -5$	$13 \equiv -4$
$11 \equiv -6$	$14 \equiv -3$	$16 \equiv -1$	$14 \equiv -3$
$16 \equiv -1$	$16 \equiv -1$		

2) Untersuchung der Zahl -1.

Rücksichtlich der Zahl -1 kann man ohne Weiteres das Theorem aufstellen: Von allen Zahlen der Form $4n+1$ ist -1 quadratischer Rest und von allen Zahlen der Form $4n-1$ ist -1 quadratischer Nichtrest. Der Beweis ergiebt sich unmittelbar durch Betrachtung der Potenz $(-1)^{\frac{p-1}{2}}$, indem im ersten Falle der Exponent derselben gerade, im zweiten Falle dagegen ungerade wird.

Wir verdanken dem berühmten Euler noch einen zweiten Beweis dieses Theoremes, welcher sich auf die Theorie der conjugirten Zahlen stützt und der hier gleichfalls einen Platz finden mag.

Sei irgend ein beliebiger quadratischer Rest r und die diesem Reste conjugirte Zahl ϱ, so folgt

$$r\varrho \equiv 1 \ (mod\ p),$$

also durch Erhebung auf die $\left(\frac{p-1}{2}\right)$ te Potenz

$$(r\varrho)^{\frac{p-1}{2}} = r^{\frac{p-1}{2}} \cdot \varrho^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

nun ist r quadratischer Rest und mithin kann man statt $r^{\frac{p-1}{2}}$ den dieser Potenz congruenten Werth 1 setzen: dadurch bekommen wir

$$\varrho^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

d. h. die Bedingungscongruenz dafür, dass ϱ ein quadratischer Rest sei, also wenn von zwei conjugirten Zahlen die eine quadratischer Rest ist, so ist es auch die andere. Demgemäss wird man die sämmtlichen $\frac{p-1}{2}$ quadratischen Reste von p in Gruppen zu je 2, die einander conjugirt sind, vertheilen können. Im Allgemeinen werden die Zahlen einer jeden Gruppe 2 von einander verschiedene Reste darstellen; doch können auch ausnahmsweise Gruppen vorkommen, welche denselben Rest zweimal enthalten. Sei die Anzahl der ersteren Gruppen b, die Anzahl der letzteren a, so ist die Anzahl sämmtlicher Reste $a+2b$ und diese muss gerade ausfallen, wenn p die Form $4n+1$ hat, dagegen ungerade, wenn p die Form $4n-1$ hat. Nun giebt es aber unter den Zahlen von 1 bis $p-1$ keine anderen Zahlen als diese beiden Grenzzahlen selbst, welche sich selbst conjugirt sind und die Zahl 1 unter diesen beiden ist auf jeden Fall quadratischer Rest, so dass sie mindestens den Werth 1 und höchstens den Werth 2 haben kann. Damit nun a im ersten Falle gerade ausfalle, muss es den Werth 2 haben, d. h. $p-1$ oder, was dasselbe ist, -1 ist quadratischer Rest, und damit es im zweiten Falle ungerade werde, muss $a=1$ sein, d. h. -1 kann nicht unter den quadratischen Resten mitzählen.

3) Untersuchung der Zahlen $+2$ und -2.

Die Betrachtung der dem Ende des vorigen Paragraphen angehängten Tabelle zeigt, dass 2 quadratischer Rest ist von den Zahlen

7 17 23 31 41 47 71 73 79 89 97,

unter denen keine von der Form $8n+3$ oder $8n-3$ sich befindet. Um diese Induction zu bewahrheiten und zugleich auf einen beliebigen (auch zusammengesetzten) ungeraden Modul auszudehnen, wollen wir annehmen, dass sich eine äusserste Grenze für den Modul p feststellen liesse, welche

durch die Zahl t repräsentirt werden möge, von der Beschaffenheit, dass 2 quadratischer Rest von t wäre, dagegen Nichtrest für alle unterhalb dieser Grenze befindlichen Modul, welche, wie t selber, eine der beiden Formen $8n+3$, $8n-3$ haben. Hiernach würde die Congruenz

$$a^2 \equiv 2 \ (mod\ t)$$

möglich sein und ihre Auflösung würde zwei Werthe für a liefern, die, wenn man die kleinsten positiven Zahlenwerthe nimmt, einander nothwendig zu dem Modul t ergänzen. Da nun t ungerade ist, so muss der eine gerade, der andere ungerade sein und man kann mithin a in der genannten Congruenz als eine bestimmbare ungerade Zahl ansehen. Dieselbe kann aber noch in doppelter Form angeschrieben werden, einmal als Gleichung wie folgt:

$$a^2-2 = ut$$

und dann als die hieraus fliessende Congruenz

$$a^2 \equiv 2 \ (mod\ u).$$

Aus letzterer ergiebt sich, dass 2 auch quadratischer Rest von u ist, aus ersterer, wie wir gleich näher zeigen wollen, dass u eine der beiden Formen $8n-3$, $8n+3$ besitzt, je nachdem t von der Form $8n+3$ oder $8n-3$ ist. Nun kann ferner die Ungleichung

$$a^2 > ut$$

wegen der anderen Ungleichung

$$a < t$$

nur so bestehen, dass man u gleichfalls kleiner als t annimmt. Dieses alles zusammengenommen würde folgen, dass, gegen die Annahme, ein Modul u kleiner als t und von einer der Formen $8n+3$, $8n-3$ existirte, von welchem 2 quadratischer Rest wäre. Also ist es unstatthaft, wenn überhaupt eine Folge von Zahlen existirt, für welche das aufgestellte Gesetz gültig ist, dieser Gültigkeit irgend eine endliche Grenze zu setzen. Nun gilt das Gesetz thatsächlich für die oben hingestellte Folge von Zahlen (die man für den Fall, dass auch zusammengesetzte Modul in Betracht kommen sollen, nach Belieben durch die erforderlichen Zwischenglieder ergänzen kann); also gilt es allgemein.

Was die behauptete Form von u anlangt, so bemerken wir, dass, da a als eine ungerade Zahl angesehen werden darf, a^2 nothwendig von der Form $8n+1$ und mithin a^2-2, d. h. der Werth des Productes ut von der Form $8n-1$ ist. Ist nun t von der $8n+3$, so muss u von der

Form $8n-3$ sein; in der That hat man unter dieser Annahme

$$ut = (8n+3)(8n'-3) = 8(8nn'+3n'-3n-1)-1,$$

d. h. ut ist, wie es sein muss, von der Form $8n-1$ und gleichzeitig wird für jede der übrigen möglichen Annahmen, dass u eine der 3 Formen

$$8n+1, \quad 8n-1, \quad 8n+3$$

habe, ut nicht die Form $8n-1$ erlangen. Ist dagegen t von der Form $8n-3$, so lässt sich in vollkommen ähnlicher Weise darthun, dass u die Form $8n+3$ habe,

Es ist jetzt erwiesen, dass 2 ein Nichtrest der Formen $8n+3$ und $8n-3$ ist. Nun ordnet sich die Form $8n+3$ der Form $4n-1$ unter; es muss mithin wegen des Satzes unter 4) *d)* im vorigen Paragraphen -2 ein Rest der Form $8n+3$ sein. Ebenso ordnet sich die Form $8n-3$ der allgemeineren Form $4n+1$ unter; zu Folge desselben Satzes ist daher -2 ein Nichtrest der Form $8n-3$. Dies zusammengefasst bekommt man das Theorem:

Die Zahl $+2$ ist ein quadratischer Nichtrest aller Primzahlen von der Form $8n+3$, die Zahl -2 dagegen ein quadratischer Rest.

Für alle Primzahlen von der Form $8n-3$ ist sowohl $+2$, wie -2 ein Nichtrest.

Durch eine ähnliche Induction findet man, dass unter den aus der Tabelle entnommenen Moduln, von welchen -2 ein Rest ist,

3 11 17 19 41 43 59 67 73 83 89 97

keiner von der Form $8n-3$ oder $8n-1$ gefunden wird. Um das Gesetz allgemein für einen beliebigen (auch zusammengesetzten) Modul von dieser Form nachzuweisen, nehme man an, dass das Gesetz für alle unterhalb der Grenze t befindlichen Modul von der vorgeschriebenen Form gültig sei, dagegen für den Modul t selbst seine Gültigkeit verliere. Dann ist wieder

$$a^2 \equiv -2 \pmod{t}$$

und diese Congruenz ist identisch mit der Gleichung

$$a^2+2 = ut,$$

sowie mit der neuen aus letzterer entspringenden Congruenz

$$a^2 \equiv -2 \pmod{u},$$

welche aussagt, dass -2 auch ein quadratischer Rest des Moduls u ist. Nun ist u wegen der Relation

$$a^2+2=ut, \quad a<t$$

kleiner als t und ferner entweder von der Form $8n-3$ oder von der Form $8n-1$. Da nämlich a immer als eine ungerade Zahl angesehen werden darf, so ist a^2 von der Form $8n+1$, also a^2+2, d. h. ut von der Form $8n+3$. Ist nun t von der Form $8n-3$, so folgt hieraus u als von der Form $8n-1$, und ist t von der Form $8n-1$, so folgt u von der Form $8n-3$. Also existirt auf jeden Fall, im Widerspruche zur Annahme, eine Zahl u kleiner als die kleinste t, welche eine der Formen $8n-3$, $8n-1$ und -2 zum quadratischen Rest hat. Da dies nicht angeht, so muss -2 ein Nichtrest zu allen Zahlen der Form $8n-3$, $8n-1$ sein. Wendet man hierauf wieder den Satz unter 4) d) in §. 14 an, so ergiebt sich dies neue Theorem, von dem indessen der erste Theil mit dem ersten Theile des vorhergehenden übereinstimmt.

Alle Primzahlen von der Form $8n-3$ haben sowohl -2, wie $+2$ zum Nichtreste.

Alle Primzahlen von der Form $8n-1$ haben -2 zum Nichtrest, dagegen $+2$ zum Reste.

Indem wir die Primzahlen nach dem Modul 8 eintheilen, ist die Form $8n+1$ bisher noch nicht zur Erörterung gekommen. Rücksichtlich derselben gilt der Satz:

Alle Primzahlen von der Form $8n+1$ haben sowohl $+2$ wie -2 zum quadratischen Reste.

Um denselben zu erweisen nehmen wir an, es sei a eine primitive Wurzel $p=8n+1$, so ist nach dem Satze p. 109 unter b) $a^{4n} \equiv -1 \pmod p$ und diese Congruenz kann in doppelter Weise umgeschrieben werden, entweder:

$$(a^{2n}+1)^2 \equiv 2a^{2n}$$

oder

$$(a^{2n}-1)^2 \equiv -2a^{2n}.$$

Demgemäss sind sowohl $2a^{2n}$ wie $-2a^{2n}$ beides Reste von p oder $8n+1$. Nun gilt dasselbe von dem diesen beiden Zahlengrössen gemeinschaftlichen Factor a^{2n}, also nach dem Satze unten 4) c) in §. 14 muss auch sowohl $+2$, wie -2 ein Rest sein.

Hiernach ist 2 auf jeden Fall ein Nichtrest zu den Formen $8n+3$ und $8n-3$. Es ist weiter zu sehen, inwiefern, indem wir zusammengesetzte Modul zulassen, es ein Rest der Formen $8n+1$ und $8n-1$ sein kann. Betrachten wir zuerst die Form $p=8n+1$, so wird 2 für die höchste Potenz irgend eines in p enthaltenen Primfactors von der Form $8n+1$ oder $8n-1$ nach dem ersten Satze unter 2) in §. 15 auf jeden Fall quadratischer Rest sein, weil es quadratischer Rest für die erste Potenz ist; dagegen wird es für die höchste Potenz irgend eines Primfactors von einer der Formen $8n+3$, $8n-3$ aus ähnlichen Gründen Nichtrest sein; wenn also Factoren der letzten Art vorkommen, so ist 2 nach einem Satze unter 1) in §. 15 quadratischer Nichtrest von p. Gehen wir von dem Modul p zu dem Modul $2p$ über, so ist 2 ein Rest von 2; denn die Congruenz

$$x^2 \equiv 2 \pmod{2}$$

wird für jedes gerade x befriedigt; also ist 2 ein Rest von $2p$ überhaupt, wenn es ein Rest von p ist. Dagegen wenn wir weiter fort zu dem Modul $4p$ schreiten, so ist 2 keinesfalls ein Rest von dem Modul 4; denn die Congruenz

$$x^2 \equiv 2 \pmod{4}$$

ist unmöglich; also ist 2 ein Nichtrest zu jeder durch 4 theilbaren Zahl. Nehmen wir in ähnlicher Weise auch die 3 noch übrigen Formen durch, so erhält man ohne Schwierigkeit folgendes Theorem, welches alle früheren in dieser Nummer als specielle Fälle in sich begreift:

Die Zahl $+2$ ist ein Rest aller solcher, sei es einfacher oder zusammengesetzter, Modul, welche weder durch 4 noch durch irgend einen Primfactor von der Form $8n+3$, $8n-3$ getheilt werden können, von den übrig bleibenden Moduln ist sie Nichtrest.

Die Zahl -2 ist ein Rest jedes beliebigen Moduls, welcher weder durch 4, noch durch irgend einen Primfactor von der Form $8n-3$ oder $8n-1$ getheilt werden kann; von allen übrig bleibenden Moduln ist sie Nichtrest.

Zwei conjugirte Zahlen sind immer zu gleicher Zeit entweder Reste oder Nichtreste. Nimmt man nun p sich wieder als eine ungerade Primzahl an, so ist die mit 2 conjugirte Zahl

$$\frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod{p}$$

und man kann die für 2 gewonnenen Resultate sofort auf die Zahl $\frac{p+1}{2}$ und $-\frac{p-1}{2}$ übertragen. Diese Uebertragung ist der besseren Uebersicht halber in folgender Tabelle enthalten:

p	$\frac{p+1}{2} \equiv -\frac{p-1}{2}$		$-\frac{p+1}{2} \equiv \frac{p-1}{2}$	
$8n+1$	$4n+1 \equiv -4n$	QR	$-(4n+1) \equiv 4n$	QR
$8n+3$	$4n+2 \equiv -(4n+1)$	NQR	$-(4n+2) \equiv 4n+1$	QR
$8n-3$	$4n-2 \equiv -(4n-1)$	NQR	$-(4n-2) \equiv 4n-1$	NQR
$8n-1$	$4n \equiv -(4n-1)$	QR	$-4n \equiv 4n-1$	NQR

Wie man sieht, ist bei dieser Uebertragung die Auflösbarkeit des Problems vorausgesetzt, zu irgend einer gegebenen Zahl q nach einem Modul p von der Form $qn \pm r$, wo n eine unbestimmte und r eine gegebene ganze Zahl bezeichnet, die conjugirte Zahl zu bestimmen. Man löse sich zu diesem Zwecke die Congruenz

$$\pm rx \equiv -1 \pmod{q}$$

auf, so ist der Quotent

$$\frac{\pm rx+1}{q}$$

eine ganze Zahl und mithin auch der Ausdruck

$$y = \frac{qmx \pm rx+1}{q} = mx + \frac{\pm rx+1}{q}.$$

Zugleich ist y die gesuchte zu q conjugirte Zahl, weil die Congruenz

$$qy = qmx \pm rx+1 \equiv 1 \pmod{p}$$

offenbar besteht.

Das vorgelegte Problem ist unmöglich, wenn q einen Theiler mit r gemeinschaftlich hat; in allen übrigen Fällen ist es möglich.

Beispiel. Die Reihe der ungeraden Primzahlen lässt sich nach dem Modul 20 in 8 Klassen eintheilen, welche durch die Zahlformen

$$20n+1 \quad 20n+3 \quad 20n+7 \quad 20n+9$$
$$20n-9 \quad 20n-7 \quad 20n-3 \quad 20n-1$$

ihre Bestimmung erhalten. Indem wir diese verschiedenen Formen nach

einander als Modul annehmen, bekommen wir für die Zahl 5 als die ihr conjugirte Zahl respective

$$\begin{array}{cccc} -4n & -(8n+1) & 8n+3 & 4n+2 \\ -(4n-2) & -(8n-3) & 8n-1 & 4n. \end{array}$$

4) Untersuchung der Zahlen $+3$ und -3.

Nehmen wir den Modul p als eine Primzahl von der Form $3n+1$, so ist 3 ein Theiler von $p-1$ und es existirt also jedenfalls eine (ungerade) Zahl h, welche zu dem Exponenten 3 gehört. Dann besteht die auf h bezügliche Restperiode aus den Potenzresten von $1, h, h^2$ und es ist zu Folge des Satzes unter 4) f) in §. 11

$$1+h+h^2 \equiv 0 \ (mod\ p).$$

Multipliciren wir diese Congruenz mit 4 und subtrahiren auf beiden Seiten 3, so erhält sie die Form

$$(2h+1)^2 \equiv -3 \ (mod\ p),$$

d. h. die Congruenz

$$x^2 \equiv -3 \ (mod\ p)$$

ist möglich oder -3 ist ein quadratischer Rest von p.

Nehmen wir dagegen p als eine ungerade Primzahl von der Form $3n+2$ an, so ist -3 ein Nichtrest. Denn nähme man an, es wäre Rest, so hiesse dies die Möglichkeit der Congruenz

$$x^2 \equiv -3 \ (mod\ p)$$

setzen und eine Wurzel derselben könnte immer als eine ungerade Zahl $< p$ bestimmt werden, so dass sie die Form $2h+1$ hätte. Also wäre

$$(2h+1)^2 \equiv -3 \ (mod\ p)$$

und hieraus würde folgen

$$1+h+h^2 \equiv 0 \ (mod\ p).$$

Multiplicirt man diese diese Congruenz auf beiden Seiten mit $h-1$, so wird

$$h^3-1 \equiv 0 \ (mod\ p)$$

und es müsste hiernach 3 ein Factor von $p-1$ sein, was gegen die Voraussetzung streitet, dass p die Form $3n+2$ hat. Also gilt das Theorem:

Zu allen Primzahlen von der Form $3n+1$ ist -3 ein Rest und zu allen Primzahlen von der Form $3n+2$ (oder $3n-1$) ist es Nichtrest.

Betrachtet man jetzt die Zahl $+3$, so muss sie für diejenigen Primzahlen $3n+1$, welche zugleich die Form $4n+1$ haben, quadratischer Rest

sein, weil -3 ebenfalls quadratischer Rest ist. Dies giebt die Form $12n+1$, welche alle diejenigen Zahlen umfasst, welche sowohl nach dem Modul 3, wie nach dem Modul 4 den Rest 1 geben. Für diejenigen Primzahlen dagegen, welche zu gleicher Zeit die Form $3n+1$ und $4n-1$ haben, d. h. von der Form $12n-5$ sind (denn dies ist die Form derjenigen Zahlen, welche nach dem Modul 3 den Rest 1 und nach dem Modul 4 den Rest -1 lassen), ist 3 Nichtrest. Betrachten wir weiter die Primzahlen von der Form $3n+2$, so können dieselben entweder von der Form $4n+1$ oder von der Form $4n-1$ sein; dem ersteren Falle entspricht die Form $12n+5$ und die Zahl 3 als Nichtrest; dem 2ten Falle die Form $12n-1$ und die Zahl 3 als Rest. Hiermit können wir folgendes Theorem aufstellen:

Die Zahl 3 ist Rest von allen Moduln der Form $12n+1$ und $12n-1$; dagegen Nichtrest von allen Moduln der Form $12n+5$ und $12n-5$.

Der letzte Satz findet also seine Ableitung aus dem vorangehenden, welcher noch eine zweite merkwürdige Ausdrucksart gestattet. Nämlich die Zahl 3 hat zu quadratischen Resten alle Zahlen, welche mit 1 congruent sind, also namentlich auch die Primzahlen von der Form $3n+1$, von denen wiederum -3 ein Rest; dagegen hat sie zu quadratischen Nichtresten alle Zahlen, die der Zahl 2 congruent sind, d. h. namentlich auch alle Primzahlen von der Form $3n+2$, von denen wiederum -3 Nichtrest ist. Dies vorausgesetzt nimmt der in Rede stehende Satz folgende Form an:

Die Zahl -3 ist quadratischer Rest aller Primzahlen, von denen selbst wieder 3 quadratischer Rest ist und quadratischer Nichtrest aller Primzahlen, von denen selbst wieder 3 Nichtrest ist.

Nach der Bezeichnungsweise von Legendre ausgedrückt giebt dies zunächst

$$\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$$

und hieraus folgt:

$$\left(\frac{3}{p}\right)=\pm\left(\frac{p}{3}\right);$$

nämlich das obere Vorzeichen gilt, wenn p die Form $4n+1$ hat, in welchem Falle

$$\left(\frac{-3}{p}\right) = (-3)^{2n} = 3^{2n} = \left(\frac{3}{p}\right),$$

und das untere Vorzeichen gilt, wenn p die Form $4n-1$ hat, in welchem Falle

$$\left(\frac{-3}{p}\right) = (-3)^{2n-1} = -3^{2n-1} = -\left(\frac{3}{p}\right)$$

ist.

Die auf die Zahlen 3 und -3 bezüglichen Sätze lassen sich sämmtlich auf die diesen Zahlen conjugirten Zahlen übertragen und wir erhalten dadurch, wenn wir bemerken, dass die Zahlen 3 und -3 nach den Moduln $12n+1$, $12n+5$, $12n-5$, $12n-1$ respective die Zahlen $-4n$ und $+4n$, $4n+2$ und $-(4m+2)$, $-(4n-2)$ und $4n-2$, $4n$ und $-4n$ conjugirt sind, folgende Tabelle:

p	3	-3				
$12n+1$	QR	QR	$-4n$	QR	$+4n$	QR
$12n+5$	NQR	NQR	$4n+2$	NQR	$-(4n+2)$	NQR
$12n-5$	NQR	QR	$-(4n-2)$	NQR	$4n-2$	QR
$12n-1$	QR	NQR	$4n$	QR	$-4n$	NQR

5) Untersuchung der Zahlen $+5$ und -5.

Sei p eine Primzahl von der Form $5n+1$, so kann immer eine ungerade Zahl h bestimmt werden, welche zu dem Exponenten 5 gehört und die auf diese Zahl h bezügliche Restperiode

$$1 \quad h \quad h^2 \quad h^3 \quad h^4$$

muss eine Reihe bilden, deren Summe ein Vielfaches von p ist, also

$$h^4+h^3+h^2+h+1 \equiv 0 \pmod{p}.$$

Multiplicirt man diese Congruenz mit 4, so gestattet die linke Seite die Form:

$$\begin{aligned} 4h^4+4h^3+4h^2+4h+4 & \\ &= 4(h+1)^4-12h(h+1)^2+4h^2 \\ &= 4(h+1)^4-12h(h+1)^2+9h^2-5h^2 \\ &= (2(h+1)^2-3h)^2-5h^2 \\ &= (2h^2+h+2)^2-5h^2 \end{aligned}$$

und die ganze Congruenz lässt sich daher schreiben wie folgt:

$$(2h^2+h+2)^2 \equiv 5h^2 \ (mod\ p),$$

woraus hervorgeht, dass $5h^2$ ein quadratischer Rest des Moduls ist. Dies setzt, da h^2 gleichfalls ein quadratischer Rest ist, voraus, dass es auch 5 sei. Denn die Zahl h ist zu Folge der Art ihrer Bestimmung von 0 verschieden, d. h. relative Primzahl zu p; mithin ist in den beiden Bedingungscongruenzen

$$(5h^2)^{\frac{p-1}{2}} = 5^{\frac{p-1}{2}},\ h^{p-1} \equiv 1 \ (mod\ p)$$

und

$$(h^2)^{\frac{p-1}{2}} = h^{p-1} \equiv 1 \ (mod\ p)$$

einmal kein Widerspruch und dann können sie nur so zusammen bestehen, wenn man

$$5^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$$

hat. Diese Schlussfolgerung ist in Uebereinstimmung mit dem Satze unter 4) c) im vorigen §.

Mithin ist bewiesen, dass 5 ein Rest jeder Primzahl von der Form $5n+1$ ist, aber es lässt sich nicht, nach Analogie der vorigen Nummer, auch das Umgekehrte zeigen, dass es von jeder Primzahl von anderer Form ein Nichtrest sei; vielmehr es lässt sich darthun, dass es von allen Primzahlen der Form $5n+4$ Rest sei. Der Beweis, welcher, wie der vorhergehende, von Lagrange herrührt, beruht auf ganz anderen Principien als der vorige und geht von der Betrachtung des Ausdruckes

$$X = \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}}$$

aus, welcher, wenn man ihn entwickelt, eine ganze rationale Function $p$ten Grades von x darstellt, nämlich er wird gleich

$$\frac{p+1}{1} \cdot 2x^p + \frac{(p+1)p(p-1)}{1.2.3} 2x^{p-2}b + \frac{(p+1)p(p-1)(p-2)(p-3)}{1.2.3.4.5} 2x^{p-4}b^2$$
$$+ \ldots\ldots + \frac{(p+1)p(p-1)}{1.2.3} 2x^3 b^{\frac{p-3}{2}} + \frac{p+1}{1} 2xb^{\frac{p-1}{2}}$$

und es erhellt, dass alle seine Glieder, bis aufs erste und letzte, da p als eine Primzahl vorausgesetzt wird, durch den Factor p ohne Rest sich theilen lassen. Die beiden übrig bleibenden Glieder lassen sich, wie folgt, zusammen schreiben:

$$2(p+1)\left(x^p + xb^{\frac{p-1}{2}}\right)$$

und sind, in der Voraussetzung, dass b ein quadratischer Nichtrest von p ist, gleichfalls ein Vielfaches von p; denn aus den Congruenzen

$$x^p \equiv x \pmod{p}$$

und

$$b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

ergiebt sich

$$x^p + xb^{\frac{p-1}{2}} \equiv x - x \equiv 0 \pmod{p}.$$

Hiernach ist

$$X \equiv 0 \pmod{p}$$

und diese Congruenz identisch mit der folgenden

$$x^p + xb^{\frac{p-1}{2}} \equiv 0 \pmod{p},$$

welche für jeden beliebigen ganzzahligen Werth von x befriedigt wird, und daher die p von einander verschiedenen Lösungen

$$x \equiv 0\ 1\ 2\ 3\ 4 \ldots\ldots p-1 \pmod{p}$$

zulässt.

Betrachten wir weiter irgend einen beliebigen Theiler e von $p+1$, so dass man $ee' = p+1$ hat, so ist der Ausdruck

$$X' = \frac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$$

gleichfalls eine ganze rationale und in X aufgehende Function von x; denn es ist

$$\frac{X}{X'} = \frac{((x+\sqrt{b})^e)^{e'} - ((x-\sqrt{b})^e)^{e'}}{(x+\sqrt{b})^e - (x-\sqrt{b})^e}$$

und die Division rechts muss nach einem bekannten Fundamentalsatze der niederen Analysis aufgehen, sobald, wie es hier eintritt, e' ein ganzer positiver Exponent ist. Daraus folgt weiter, dass man sich den Ausdruck X in 2 Factoren X' und X'' zerlegen kann, von denen der erste den Grad $e-1$, der zweite den Grad $p-e+1$ hat, so dass also

$$X = X'X''$$

ist. Ferner müssen die Wurzeln der Congruenz $X \equiv 0 \pmod{p}$ identisch sein mit den Wurzeln der Congruenzen

$$X' \equiv 0,\ X'' \equiv 0 \pmod{p},$$

von denen die erste höchstens $e-1$, die zweite höchstens $p-e+1$ Lö-

sungen hat. Da nun beide zusammen mit Nothwendigkeit p reelle Lösungen haben, so ist die höchste Zahl der möglichen Lösungen in unserem Falle auch zugleich die wirklich existirende und es giebt also $e-1$ Zahlenwerthe, für welche der Ausdruck X' der 0 congruent oder mit anderen Worten durch p theilbar wird.

Nehmen wir nun p als von der Form $5n+4$ an, so wird 5 ein Theiler von $p+1$ und die Congruenz

$$\frac{(x+\sqrt{b})^5-(x-\sqrt{b})^5}{\sqrt{b}} \equiv 0 \ (mod\ p)$$

ist möglich und zwar wird sie durch 4 verschiedene Zahlenwerthe von x befriedigt. Nun giebt dieselbe durch die Entwickelung der Potenzen im Zähler:

$$10x^4+20x^2b+2b^2 \equiv 0 \ (mod\ p)$$

und diese Congruenz ist identisch mit der folgenden:

$$(5x^2+b)^2 \equiv 20x^4 \ (mod\ p).$$

Da dieselbe nun möglich ist, so ist $20x^4$ ein Rest von p und sondern wir hiervon den Factor $4x^4$, der auf jeden Fall gleichfalls ein Rest und zwar ein von 0 verschiedener ist, ab, so folgt 5 auch als quadratischer Rest. — Die Annahme eines von 0 verschiedenen x ist hierbei statthalt. Denn wäre x ein Vielfaches von p, so folgte aus der Congruenz

$$10x^4+20x^2b+2b^2 \equiv 0$$

die neue

$$2b^2 \equiv 0 \ (mod\ p),$$

welche nur bestehen kann, wenn b der 0 congruent und mithin der Annahme zuwider ein Rest ist. Sie ist aber zugleich auch nothwendig, weil der letzte Schluss, der auf dem Satz unter 4) c) im vorigen §. beruht, sonst nicht Geltung haben könnte.

Es bleibt noch übrig die Formen $5n+2$ und $(5n+3 \equiv)$ $5n-2$ zu untersuchen, rücksichtlich deren vermöge der Tabelle erhellt, dass 5 ein Nichtrest sei, wenigstens bis zur Grenze 97 hin. Nehmen wir an, es gäbe solche Modul, die diese Form besässen und doch 5 zum Reste hätten, und sei der kleinste darunter t, so ist die Congruenz

$$a^2 \equiv 5 \ (mod\ t)$$

möglich und 5 von allen Moduln unterhalb der Grenze t Nichtrest. Nun kann man aber diese Congruenz sich auch als die Gleichung

$$a^2 = 5+tu$$

schreiben und hierin a als eine gerade Zahl $< t$ annehmen: dann folgt,

dass u eine ungerade Zahl und gleichfalls kleiner als t sei. Da man ferner gemäss der vorhergehenden Gleichung

$$a^2 \equiv tu \ (mod\ 5)$$

hat, so muss tu ein Rest von 5 sein. Es ist aber zugleich t ein Nichtrest von 5; denn t ist von der Form

$$5n \pm 2 \equiv \pm 2 \ (mod\ 5)$$

und sowohl $+2$, wie -2 ein Nichtrest von 5. Also kann tu nur so Rest von 5 sein, dass man u gleichzeitig als Nichtrest von 5 hat. Dies setzt die Congruenz

$$u \equiv \pm 2 \ (mod\ 5)$$

voraus, d. h. u muss eine der beiden Formen $5n+2$ oder $5n-2$ haben. Wenn hier u eine Primzahl sein sollte, so tritt der Widerspruch mit der Annahme sofort klar hervor; denn vermöge der obigen Gleichung ist

$$a^2 \equiv 5 \ (mod\ u)$$

und daher 5 ein Rest von u; es existirte also ein Modul kleiner als t und Primzahl von der Form $5n \pm 2$, von welchem 5 Rest wäre. Aber auch wenn u eine zusammengesetzte Zahl ist, lässt sich der nämliche Widerspruch aufzeigen; denn wenn 5 ein Rest von u ist, so muss es auch von jedem Primfactor der Grösse u ein Rest sein und da u ungerade und von der Form $5n \pm 2$ ist, so kann es sich nicht aus lauter Primfactoren der Form $4n \pm 1$ zusammensetzen, sondern es muss wenigstens einen ungeraden Primfactor der Form $5n \pm 2$ haben. Für diesen Primfactor mithin $< t$ und von der genannten Form wäre 5 gleichfalls quadratischer Rest.

Hiernach können wir folgendes Theorem aussprechen:

Die Zahl 5 ist ein Rest aller Primzahlen von der Form $5n \pm 1$, dagegen ein Nichtrest aller Primzahlen von der Form $n5 \pm 2$.

Bemerken wir, dass alle Zahlen der Form $5n \pm 1$ in Bezug auf den Modul 5 congruent mit ± 1 und daher quadratische Reste von 5 sind, sowie dass alle Zahlen von der Form $5n \pm 2$ quadratische Nichtreste von 5 sind, so können wir unserem Theoreme die elegante Aussprache geben:

Die Zahl 5 ist quadratischer Rest von allen solchen Primzahlen, die es selber in Bezug auf 5 als Modul sind, und quadratischer Nichtrest von allen solchen Primzahlen, die es selber in Bezug auf 5 als Modul sind.

Nach Legendres Bezeichnung drückt sich dies in der folgenden Gleichung aus:

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right).$$

Schliessen wir in der gewöhnlichen Weise weiter auf —5, so erhalten wir folgende Tabelle:

p	5	—5
$20n+1$	*QR*	*QR*
$20n+3$	*NQR*	*QR*
$20n+7$	*NQR*	*QR*
$20n+9$	*QR*	*QR*
$20n-9$	*QR*	*NQR*
$20n-7$	*NQR*	*NQR*
$20n-3$	*NQR*	*NQR*
$20n-1$	*QR*	*NQR*

Dehnen wir endlich die gewonnenen Resultate auf die mit 5 und —5 conjugirten Zahlen aus, so kommen folgende Resultate:

p	5		—5	
$20n+1$	$-4n$	*QR*	$4n$	*QR*
$20n+3$	$-(8n+1)$	*NQR*	$8n+1$	*QR*
$20n+7$	$8n+3$	*NQR*	$-(8n+3)$	*QR*
$20n+9$	$4n+2$	*QR*	$-(4n+2)$	*QR*
$20n-9$	$-(4n-2)$	*QR*	$4n-2$	*NQR*
$20n-7$	$-(8n-3)$	*NQR*	$8n-3$	*NQR*
$20n-3$	$8n-1$	*NQR*	$-(8n-1)$	*NQR*
$20n-1$	$4n$	*QR*	$-4n$	*NQR*

6) Untersucht man weiter die Zahlen +7 und —7, so findet man durch eine aus der Tabelle des vorigen Paragraphen geschöpfte Induction den Satz:

Die Zahl —7 ist ein Rest jeder Primzahl, welche selber ein Rest von 7 ist, d. h. eine der 3 Formen $7n+1$, $7n-3$, $7n-2$ hat.

Die Zahl —7 ist ein Nichtrest jeder Primzahl, welche selber ein Nichtrest von 7 ist, d. h. eine der 3 Formen $7n-1$, $7n+3$, $7n+2$ hat.

Nach Legendres Bezeichnung giebt dies

$$\left(\frac{-7}{p}\right)=\left(\frac{p}{-7}\right)$$

und wenn man in der bekannten Weise von -7 zu dem Reste $+7$ übergeht, so findet man nach derselben Manier der Bezeichnung, je nachdem p die Form $4n+1$ oder $4n-1$ hat, die Relation

$$\left(\frac{7}{p}\right)=\pm\left(\frac{p}{7}\right).$$

Der Beweis ist ziemlich schwierig und weitläufig. Dazu kommt, dass die bisherigen Mittel der Demonstration nicht für alle Fälle ausreichen und daher die Nothwendigkeit eintritt sich nach neuen umzusehen. Wir wollen daher nicht näher darauf eingehen und zu der allgemeinen Betrachtung mit dem Bemerken fortschreiten, dass die von uns betrachteten speciellen Fälle das Stattfinden folgenden Gesetzes anzudeuten scheinen:

Wenn q und p beide Primzahlen von der Form $4n-1$ sind, so findet die Relation

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$$

statt; wenn dagegen nicht beide zugleich von dieser Form sind, so besteht die Relation

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

Das ist das berühmte Reciprocitätsgesetz in der Form, die ihm von Legendre gegeben ist; Gauss dagegen, der der erste war, der es bewies und im Ganzen nicht weniger als 6 von einander sehr verschiedene und alle sehr bemerkenswerthe Beweise geliefert hat, spricht das Fundamentaltheorem in folgender Form aus:

Je nachdem q als eine Primzahl von der Form $4n+1$ oder $4n-1$ sich bestimmt, ist $+q$ oder $-q$ quadratischer Rest oder Nichtrest jeder (positiv genommenen) Primzahl p, welche selber wieder quadratischer Rest oder Nichtrest der ersten Primzahl q ist.

§. 17.

Der Satz der Reciprocität.

1) Der besseren Uebersicht wegen wollen wir dem Hauptbeweise einige einleitende Sätze vorausschicken, was um so zweckmässiger erscheint, da dieselben ein eigenthümliches Interesse für sich selber in Anspruch nehmen. Der erste ist folgender:

Wenn p eine Primzahl ist und q eine nicht durch p theilbare Zahl, so sind die Reste

$$1q \quad 2q \quad 3q \quad 4q \quad \ldots\ldots \frac{p-1}{2}q$$

in Bezug auf den Modul p alle von einander verschieden. Diese Reste werden, wenn wir sie alle positiv nehmen, zum Theil grösser, zum Theil kleiner als $\frac{p}{2}$ ausfallen. Sei nun die Anzahl derjenigen, welche grösser als $\frac{1}{2}p$ sind, gleich μ, so findet immer der Satz statt:

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) = (-1)^{\mu} \ (mod\ p),$$

d.h. es ist q quadratischer Rest oder Nichtrest, je nachdem μ gerade oder ungerade ist.

Nehmen wir z. B. $p = 17$, $q = 3$, so werden die Reste sämmtlicher Glieder der Reihe

$$3 \quad 6 \quad 9 \quad 12 \quad 15 \quad 18 \quad 21 \quad 24$$

nach dem Modul 17 bezüglich congruent mit den Resten

$$3 \quad 6 \quad 9 \quad 12 \quad 15 \quad 1 \quad 4 \quad 7;$$

diejenigen darunter, welche grösser als $\frac{1}{2}p = 8\frac{1}{2}$, sind

$$9 \quad 12 \quad 15$$

und ihre Anzahl μ ist gleich 3. Also ist 3 quadratischer Nichtrest von 17.

Setzen wir dagegen $q = 8$, so ist die Productenreihe

$$8 \quad 16 \quad 24 \quad 32 \quad 40 \quad 48 \quad 56 \quad 64$$

und die entsprechende Restreihe

$$8 \quad 16 \quad 7 \quad 15 \quad 6 \quad 14 \quad 5 \quad 13;$$

die Reste hierunter, die grösser als $8\frac{1}{2}$, sind 16, 15, 14, 13; also $\mu = 4$ und 8 quadratischer Rest von 17.

Sei jetzt allgemein

$$(A) \quad a' \quad a'' \quad a''' \quad \ldots\ldots \quad a^{(\nu)}$$

die Reihe der Reste, welche kleiner und

$$b' \quad b'' \quad b''' \quad \ldots\ldots \quad b^{(\mu)}$$

die Reihe der Reste, welche grösser als $\frac{1}{2}p$ sind: dann ist die letzte Restreihe gleichgeltend mit der folgenden:

$$(B) \quad -(p-b') \quad -(p-b'') \quad \ldots\ldots\ldots \quad -(p-b^{(\mu)}),$$

welche lauter negative Reste enthalten wird, während die Reihe (A) lauter positive kleinste Reste in sich schliesst. Mithin kommt in beiden Reihen kein Rest vor, der nicht kleiner als $\frac{1}{2}p$ wäre. Zu gleicher Zeit kann aber auch behauptet werden, dass die absoluten Werthe der Reste in (A) nicht blos unter einander verschieden sind, sondern auch verschieden sind von den absoluten Werthen der Reste in (B). Denn wären irgend welche zwei einander gleich, etwa

$$a^{(n)} = p - b^{(m)},$$

so folgte, wenn man unter Nq dasjenige Glied unserer Productenreihe versteht, welches dem Reste $a^{(n)}$, und unter Mq dasjenige Glied, welches dem Reste $b^{(m)}$ entspricht, die Congruenz

$$Nq \equiv -Mq \pmod{p},$$

also

$$(N+M)q \equiv 0 \pmod{p}$$

und da q und p relative Primzahlen sind, so kann diese Congruenz nur so bestehen, dass man

$$N+M \equiv 0 \pmod{p}$$

hat, d. h. $N+M$ müsste ein Vielfaches von p sein, was unmöglich ist, da M und N beides Zahlen sind, die für sich kleiner als $\frac{p}{2}$.

Die Reste der Reihen (A) und (B) haben also verschiedene absolute Werthe und sind alle kleiner als $\frac{1}{2}p$. Da nun die Anzahl der in beiden vorkommenden Reste $\frac{p-1}{2}$ ist, so kann dies nur dann eintreten, wenn diese absoluten Werthe, wenn auch vielleicht in anderer Folge, mit der Reihe der Zahlen

$$1 \quad 2 \quad 3 \quad \ldots\ldots \quad \frac{p-1}{2}$$

übereinstimmen. Hiernach ist nothwendig das Restproduct

$$(-1)^{\mu} . a'a''a''' \ldots\ldots a^{(\nu)} . (p-b') . (p-b'') \ldots\ldots (p-b'^{(\mu)})$$
$$= (-1)^{\mu} . 1 . 2 . 3 \ldots . \frac{p-1}{2}.$$

Nun ist aber die linke Seite dieser Gleichung das Product sämmtlicher Reste, die in den beiden Reihen (A) und (B) enthalten sind, und mithin zu Folge unserer Voraussetzung nach dem Modul p congruent dem Producte

$$1q . 2q . 3q . 4q \ldots\ldots \frac{p-1}{2} q = 1 . 2 . 3 . 4 \ldots . \frac{p-1}{2} q^{\frac{p-1}{2}}.$$

Setzt man dies ein, so erhält man die Congruenz

$$1 . 2 . 3 . 4 \ldots . \frac{p-1}{2} q^{\frac{p-1}{2}} \equiv (-1)^{\mu} . 1 . 2 . 3 \ldots . \frac{p-1}{2} \; (mod\ p)$$

oder, wenn man den Factor $1 . 2 . 3 . 4 \ldots . \frac{p-1}{2}$, der auf beiden Seiten vorkommt und auf jeden Fall eine relative Primzahl zu dem Modul p ist, herausdividirt:

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) = (-1)^{\mu} \; (mod\ p).$$

Der eben bewiesene Satz giebt ein neues Mittel an die Hand die Formen des Moduls p zu bestimmen, von welchen die Zahlen 2, -2, -1 Reste oder Nichtreste sind. Wir begnügen uns in einem einzelnen Falle die Möglichkeit zu zeigen und die Durchführung der übrigen möglichen Fälle dem Leser zu überlassen. Nehmen wir also

$$p = 8n+1, \; q = 2;$$

so ist die Reihe der in Betracht kommenden Producte

$$1.2 \quad 2.2 \quad 3.2 \; \ldots\ldots \; 2n.2 \quad (2n+1).2 \quad (2n+2).2 \; \ldots\ldots \; (2n+2n).2$$

und es springt sofort in die Augen, dass die erste Hälfte dieser Producte bis zu $2n.2$ incl. kleiner, die zweite Hälfte dagegen grösser als $\frac{1}{2}p$ ist, kein einziges aber den Modul p übersteigt, so dass die Reihe der Producte und die Reihe der Reste hier in eine einzige zusammenfallen. Die Anzahl der in der letzten Hälfte vorkommenden Reste ist nun offenbar $2n$, also $\mu = 2n$ und zu Folge unseres Satzes geht daraus hervor, dass 2 ein quadratischer Rest der Form $8n+1$ ist.

2) Bezeichnen wir nach dem Vorgange von Legendre durch $E\left(\frac{x}{p}\right)$ die höchste Anzahl der Ganzen, welche in dem Bruche $\frac{x}{p}$ enthalten ist,

so wird, wenn man unter r den gewöhnlichen positiven Divisionsrest versteht, immer die Gleichung

$$x = pE\left(\frac{x}{p}\right) + r$$

Bestand haben. Betrachtet man nun die Reihe der Producte

$$1q \quad 2q \quad 3q \quad 4q \quad \ldots\ldots\ldots \quad \frac{p-1}{2}q$$

und mögen wieder in Bezug auf den Modul p

$$a' \quad a'' \quad a''' \quad \ldots\ldots \quad a^{(\nu)}$$

die Reste sein, welche kleiner als der halbe Modul, und

$$b' \quad b'' \quad b''' \quad \ldots\ldots \quad b^{(\mu)}$$

die Reste, welche grösser als der halbe Modul sind; ferner seien die diesen Resten entsprechenden Vielfachen von q respective

$$A'q \quad A''q \quad A'''q \quad \ldots\ldots \quad A^{(\nu)}q,$$
$$B'q \quad B''q \quad B'''q \quad \ldots\ldots \quad B^{(\mu)}q$$

und endlich M die Summe der sämmtlichen E, welche bei der Division dieser Vielfachen durch p herauskommen, so ist

$$M = E\left(\frac{q}{p}\right) + E\left(\frac{2q}{p}\right) + E\left(\frac{3q}{p}\right) + \ldots + E\left(\frac{\frac{p-1}{2}q}{p}\right),$$

und insofern es bei unserer Untersuchung wesentlich darauf ankommt zu finden, ob μ gerade oder ungerade ist, ist es immer zulässig an Stelle der Zahl μ die Zahl M zu betrachten. Das Nähere hierüber sagt folgendes Theorem:

Wenn p eine beliebige ungerade Primzahl und q eine gleichfalls ungerade Zahl bezeichnet, die kein Vielfaches von p ist, so ist die Anzahl μ der Reste $> \frac{1}{2}p$, welche bei der Division der Vielfachen

$$1q \quad 2q \quad 3q \quad 4q \quad \ldots\ldots \quad \frac{p-1}{2}q$$

durch den Modul p hervorgehen, gleichzeitig gerade oder ungerade mit der Summe M der sämmtlichen E, die sich bei der angedeuteten Division ergeben, oder in Zeichen, es ist

$$M \equiv \mu \ (mod\ 2).$$

Zu Folge der obigen Erklärungen ist allgemein

$$\frac{Aq}{p} - E\left(\frac{Aq}{p}\right) < \tfrac{1}{2},$$

$$\frac{Bq}{p} - E\left(\frac{Bq}{p}\right) > \tfrac{1}{2}, \text{ aber } < 1;$$

mithin, wenn wir beide Ungleichungen mit 2 multipliciren:

$$\frac{2Aq}{p} - 2E\left(\frac{Aq}{p}\right) < 1,$$

$$\frac{2Bq}{p} - 2E\left(\frac{Bq}{p}\right) > 1, \text{ aber } < 2;$$

also folgt, wenn wir uns nur auf die Ganzen beschränken,

$$E\left(\frac{2Aq}{p}\right) - 2E\left(\frac{Aq}{p}\right) = 0,$$

$$E\left(\frac{2Bq}{p}\right) - 2E\left(\frac{Bq}{p}\right) = 1.$$

Denken wir uns nun für A und B alle nur möglichen Werthe eingesetzt, so sind die verschiedenen A und B durcheinander genommen alle nur möglichen Zahlen von 1 bis $\frac{p-1}{2}$ und wir bekommen daher, indem wir alles zusammennehmen, wenn wir berücksichtigen, dass die Zahl der B gleich μ ist,

$$\left.\begin{matrix} E\left(\frac{2q}{p}\right) + E\left(\frac{4q}{p}\right) + E\left(\frac{6q}{p}\right) + \ldots\ldots + 2E\left(\frac{(p-1)q}{p}\right) \\ -2E\left(\frac{q}{p}\right) - 2E\left(\frac{2q}{p}\right) - 2E\left(\frac{3q}{p}\right) - \ldots\ldots - 2E\left(\frac{\frac{p-1}{2}q}{p}\right) \end{matrix}\right\} = \mu.$$

Die untere Zahlenreihe giebt offenbar eine (negativ genommen) gerade Zahl; wir können also mit deren Weglassung schreiben:

$$E\left(\frac{2q}{p}\right) + E\left(\frac{4q}{p}\right) + E\left(\frac{6q}{p}\right) + \ldots\ldots + E\left(\frac{(p-1)q}{p}\right) \equiv \mu \pmod 2.$$

Betrachten wir jetzt irgend ein specielles Glied links, etwa

$$E\left(\frac{(p-r)q}{p}\right)$$

und setzen zu dem Zwecke

$$q = mp + n,$$

wo n den gewöhnlichen Divisonsrest von q durch p bezeichnet, so ist doch

$$\frac{(p-r)q}{p} = q - mr - \frac{nr}{p},$$

also

$$E\left(\frac{(p-r)q}{p}\right)=E\left(q-mr-\frac{nr}{p}\right)$$

oder, da die Anzahl q der positiven Ganzen durch den Abzug des ächten Bruches, der nach Wegnahme der in $\frac{nr}{p}$ enthaltenen Ganzen übrig bleibt, auf jeden Fall um eine Einheit verringert wird,

$$=q-1-E\left(mr+\frac{nr}{p}\right).$$

Nun besteht die Gleichung

$$\frac{qr}{p}=\frac{mpr+nr}{p}$$

und hieraus folgt

$$E\frac{qr}{p}=E\left(mr+\frac{nr}{p}\right),$$

mithin geht unsere vorhergehende Gleichung über in

$$E\left(\frac{(p-r)q}{p}\right)=q-1-E\left(\frac{rq}{p}\right).$$

Denken wir uns nun in unsere letzte Congruenz für μ die letzte Hälfte der Glieder, welche die Summe auf der linken Seite hat, vermöge der vorhergehenden Formel transformirt, so sind, wenn p von der Form $4n+1$ ist, die zu transformirenden Glieder alle diejenigen, für welche der Index r die Werthe

$$r=1\quad 2\quad 3\quad 4\quad \ldots\quad \frac{p-3}{2}$$

annimmt, und ihre Anzahl ist $\frac{1}{4}(p-1)$; dagegen wenn p von der Form $4n+3$ ist, so sind diejenigen Glieder zu transformiren, für welche r die Werthe

$$r=1\quad 2\quad 3\quad 4\quad \ldots\quad \frac{p-1}{2}$$

bekommt, und ihre Anzahl ist $\frac{1}{4}(p+1)$. Mithin geht unsere Congruenz im ersten Falle über in

$$\left.\begin{array}{l}\frac{1}{4}(p-1)(q-1)+E\left(\frac{2q}{p}\right)+E\left(\frac{4q}{p}\right)+\ldots+E\left(\frac{\frac{p-1}{2}q}{p}\right)\\ \quad -E\left(\frac{q}{p}\right)-E\left(\frac{3q}{p}\right)-\ldots-E\left(\frac{\frac{p-3}{2}\cdot q}{p}\right)\end{array}\right\}\equiv\mu\ (mod\ 2)$$

und im zweiten Falle in

$$\left.\begin{array}{r}\frac{1}{4}(p+1)(q-1)+E\left(\frac{2q}{p}\right)+E\left(\frac{4q}{p}\right)+\ldots.+E\left(\frac{\frac{p-3}{2}q}{p}\right)\\ -E\left(\frac{q}{p}\right)-E\left(\frac{3q}{p}\right)-\ldots.-E\left(\frac{\frac{p-1}{2}q}{p}\right)\end{array}\right\}\equiv\mu\ (mod\ 2).$$

Addiren wir in beiden Fällen das Doppelte der jedesmaligen unteren Horizontalreihe auf der linken Seite hinzu, welches zulässig, da dies Doppelte ein Multiplum von 2 ist, und lassen im ersten Falle den Ausdruck

$$\tfrac{1}{4}(p-1)(q-1),$$

weil er gleichfalls ein Multiplum von 2 ist, und im zweiten Falle aus einem ähnlichen Grunde den Ausdruck

$$\tfrac{1}{4}(p+1)(q-1)$$

weg, so ergiebt sich in vollkommener Allgemeinheit die Congruenz:

$$E\left(\frac{q}{p}\right)+E\left(\frac{2q}{p}\right)+E\left(\frac{3q}{p}\right)+\ldots..+E\left(\frac{\frac{p-1}{2}q}{p}\right)\equiv\mu\ (mod\ 2)$$

oder einfacher, wie behauptet wurde,

$$M\equiv\mu\ (mod\ 2).$$

3) Zu Folge des vorhergehenden Satzes können wir also an Stelle der Zahl μ die Summe der verschiedenen E in Rechnung bringen und um deswillen, indem wir q und p als zwei ungerade Zahlen annehmen, von denen p die grössere ist, wollen wir den Werth dieser Summe näher in Betracht ziehen.

Setzen wir die beiden Gleichungssysteme:

$$(P)\left\{\begin{array}{ll} q=p\pi' & +r' \\ 2q=p\pi'' & +r'' \\ 3q=p\pi''' & +r''' \\ 4q=p\pi^{IV} & +r^{IV} \\ \ldots\ldots & \\ \ldots\ldots & \\ \frac{p-1}{2}q=p\pi^{\left(\frac{p-1}{2}\right)} & +r^{\left(\frac{p-1}{2}\right)} \end{array}\right. \qquad \left.\begin{array}{ll} p=q\varkappa' & +\varrho' \\ 2p=q\varkappa'' & +\varrho'' \\ 3p=q\varkappa''' & +\varrho''' \\ 4p=q\varkappa^{IV} & +\varrho^{IV} \\ \ldots\ldots & \\ \ldots\ldots & \\ \frac{q-1}{2}p=q\varkappa^{\left(\frac{q-1}{2}\right)} & +\varrho^{\left(\frac{q+1}{2}\right)} \end{array}\right\}(Q)$$

wo die Zahlen

$$\pi' \quad \pi'' \quad \pi''' \quad \ldots\ldots$$
$$\varkappa' \quad \varkappa'' \quad \varkappa''' \quad \ldots\ldots$$

respective die ganzen Zahlen

$$E\left(\frac{q}{p}\right) \quad E\left(\frac{2q}{p}\right) \quad E\left(\frac{3q}{p}\right) \;\ldots\ldots$$

$$E\left(\frac{p}{q}\right) \quad E\left(\frac{2p}{q}\right) \quad E\left(\frac{3p}{q}\right) \;\ldots\ldots$$

bezeichnen: dann ist zunächst klar, dass die letzte der Gleichungen (P) durch die Annahmen

$$\pi^{\left(\frac{p-1}{2}\right)} = \frac{q-1}{2}, \; r^{\left(\frac{p-1}{2}\right)} = \frac{p-q}{2}$$

zu einer Identität wird und dass mithin, da gleichzeitig dadurch $r^{\left(\frac{p-1}{2}\right)}$ positiv und kleiner als p ausfällt, der bezeichnete Werth von $\pi^{\left(\frac{p-1}{2}\right)}$ mit $E\left(\frac{\left(\frac{p-1}{2}\right)q}{p}\right)$ identisch ist. Ferner erhellt, dass den x' ersten Vielfachen

$$1q \quad 2q \quad 3q \;\ldots\ldots\; x'q$$

lauter $\pi = 0$ entsprechen; denn da $x'q$ zu Folge der ersten Gleichung (Q) keiner als p ist, so liegen diese Vielfachen alle zwischen den Grenzen 0 und p, so jedoch, dass keines irgend einer dieser Grenzen gleich werden könnte; mithin sind die aus ihrer Division mit p hervorgehenden Quotienten zwischen 0 und 1 enthalten, d. h. ächte Brüche und die zugehörigen Ganzen gleich 0. Geht man weiter, so ist schon das nächste Vielfache

$$(x'+1)q > p,$$

wie durch Subtraction der Ungleichung

$$\varrho' < q$$

von der aus der ersten Gleichung (Q) fliessenden Gleichung

$$(x'+1)q + \varrho' = p + q$$

erkannt wird, und die $(x''-x')$ Vielfachen

$$(x'+1)q \quad (x'+2)q \quad (x'+3)q \;\ldots\ldots\; x''q$$

sind alle wegen der ersten und zweiten Gleichung (Q) grösser als p und kleiner als $2p$; mithin sind die Quotienten dieser Vielfachen durch p zwischen den Grenzen 1 und 2, d.h. die in ihnen enthaltenen Ganzen π sind alle gleich 1. Ganz ebenso findet man, dass die $(x'''-x'')$ Vielfachen

$$(x''+1)q \quad (x''+2)q \quad (x''+3)q \;\ldots\ldots\; x'''q$$

alle grösser als $2p$ und kleiner als $3p$ und dem zu Folge die zugehörigen π gleich 2 sind. Indem man so weiter fortgeht, kommt man zuletzt zu den $\left\{\frac{p-1}{2} - \varkappa^{\left(\frac{q-1}{2}\right)}\right\}$ Vielfachen

$$\left(\varkappa^{\left(\frac{p-1}{2}\right)}+1\right)q \quad \left(\varkappa^{\frac{q-1}{2}}+2\right)q \quad \ldots\ldots \quad \frac{p-1}{2}q;$$

dieselben sind sämmtlich grösser als $\frac{q-1}{2}p$, zu Folge der letzten Gleichung (Q), und kleiner als $\frac{q-1}{2}p+p$, weil das höchste unter ihnen dieser Ungleichheit, wie man sich leicht überzeugt, Genüge leistet; mithin sind die zugehörigen π alle gleich $\frac{q-1}{2}$.

Hiernach ist, wenn man das bekannte Summenzeichen einführt,

$$\sum \pi = \varkappa'.0+(\varkappa''-\varkappa').1+(\varkappa'''-\varkappa'').2+(\varkappa^{IV}-\varkappa''').3$$
$$+\ldots\ldots+\left(\frac{p-1}{2}-\varkappa^{\left(\frac{q-1}{2}\right)}\right).\frac{q-1}{2}$$

oder, wenn man reducirt

$$=-\varkappa'-\varkappa''-\varkappa'''-\varkappa^{IV}-\ldots.-\varkappa^{\left(\frac{q-1}{2}\right)}+\frac{p-1}{2}.\frac{q-1}{2}$$
$$=-\sum\varkappa+\frac{p-1}{2}.\frac{q-1}{2},$$

also folgt die bemerkenswerthe Gleichung

$$\sum\pi+\sum\varkappa=\frac{p-1}{2}.\frac{q-1}{2}$$

oder in Worten das Theorem:

Wenn q und p zwei ungerade Zahlen sind, die keinen gemeinschaftlichen Theiler besitzen, so ist die Summe der Zahlen

$$E\left(\frac{q}{p}\right) \quad E\left(\frac{2q}{p}\right) \quad E\left(\frac{3q}{p}\right) \ldots\ldots E\left(\frac{\frac{p-1}{2}q}{p}\right)$$

zusammmengenommen mit der Summe der Zahlen

$$E\left(\frac{p}{q}\right) \quad E\left(\frac{2p}{q}\right) \quad E\left(\frac{3p}{q}\right) \ldots\ldots E\left(\frac{\frac{q-1}{2}p}{q}\right)$$

gleich dem Producte $\frac{p-1}{2}.\frac{q-1}{2}$.

4) Fassen wir die drei vorstehenden Theoreme zusammen, so ergiebt sich unmittelbar das Gesetz der Reciprocität. Wenden wir den zweiten Satz auf den dritten an, so können wir, da es blos auf den geraden oder ungeraden Zustand der in letzterem vorkommenden Summen ankommt, statt der letzteren geradezu die Zahlen μ und ν setzen und erhalten so

$$\mu+\nu \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} \ (mod\ 2);$$

gleichzeitig hat man zu Folge des ersten Satzes

$$\left(\frac{q}{p}\right)=(-1)^{\mu},$$

$$\left(\frac{p}{q}\right)=(-1)^{\nu}.$$

Seien nun die Zahlen p und q zunächst beide von der Form $4n-1$, so wird $\mu+\nu$ ungerade, d. h. es muss die eine von diesen Zahlen gerade und die andere ungerade sein; die ihnen entsprechenden Potenzen von -1 haben daher entgegengesetztes Zeichen und es ist

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right),$$

oder genauer, wenn q quadratischer Rest von p ist, d. h. wenn $\left(\frac{q}{p}\right)=1$ giebt, so ist p ein Nichtrest von q, d. h. $\left(\frac{p}{q}\right)=-1$ und umgekehrt wenn q ein Nichtrest von p ist, so ist p ein Rest von q.

Seien dagegen die Zahlen p und q entweder beide oder wenigstens eine darunter von der Form $4n+1$, so ist $\mu+\nu$ mit Nothwendigkeit eine gerade Zahl und die Zahlen μ und ν mithin entweder beide gleichzeitig gerade oder beide gleichzeitig ungerade. Demgemäss bekommt man die Reste der Potenzen $\left(\frac{q}{p}\right)$ und $\left(\frac{p}{q}\right)$ (der erste auf den Modul p, der zweite auf den Modul q bezogen) und beide entweder zugleich $+1$ oder -1 und kann dies Verhältniss symbolisch durch die Gleichung

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

ausdrücken, welche näher sagt, dass, wenn q ein Rest von p, auch p ein Rest von q oder wenn q ein Nichtrest von p, auch p ein Rest von q sei.

Wie sehr dieser Satz der Reciprocität die Untersuchung vereinfache, wollen wir an einigen durchgerechneten Beispielen zeigen.

Beispiel 1. $q = 19$, $p = 101$, also von der Form $4n+1$. Hiernach ist

$$\left(\frac{19}{101}\right) = \left(\frac{101}{19}\right) = \left(\frac{95+6}{19}\right) = \left(\frac{6}{19}\right) = \left(\frac{2}{19}\right) \cdot \left(\frac{3}{19}\right).$$

Nun ist 2 quadratischer Rest der Formen $8n \pm 1$ und quadratischer Nichtrest der Formen $8n \pm 3$; hiernach ist 2 ein Nichtrest von 19, d. h. $\left(\frac{2}{19}\right) = -1$. Ferner ist, da 19 und 3 beide von der Form $4n-1$ sind,

$$\left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Mithin wird

$$\left(\frac{19}{101}\right) = \left(\frac{2}{19}\right)\left(\frac{3}{19}\right) = -1 . -1 = 1;$$

also ist 19 ein quadratischer Rest von 101 und in der That besteht die Congruenz

$$25^2 \equiv 19 \; (mod\; 101).$$

Beispiel 2. $q = 43$, also von der Form $4n-1$; $p = 883$, also von der nämlichen Form.

$$\left(\frac{43}{883}\right) = -\left(\frac{883}{43}\right) = -\left(\frac{20.43+23}{43}\right) = -\left(\frac{23}{43}\right) = \left(\frac{-20}{43}\right) = \left(\frac{20}{43}\right);$$

$$\left(\frac{20}{43}\right) = \left(\frac{4}{43}\right) \cdot \left(\frac{5}{43}\right);$$

$$\left(\frac{4}{43}\right) = \left(\frac{2}{43}\right) \cdot \left(\frac{2}{43}\right) = -1 . -1 = +1;$$

$$\left(\frac{5}{43}\right) = \left(\frac{43}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1;$$

$$\left(\frac{43}{883}\right) = \left(\frac{4}{43}\right) \cdot \left(\frac{5}{43}\right) = +1 . -1 = -1,$$

d. h. 43 ist ein quadratischer Nichtrest von 883.

Beispiel 3. $q = 453$, $p = 1236 = 4.3.103$.

$453 \equiv 1 \; (mod\; 4)$, also 453 *QR* von 4;

$453 \equiv 0 \; (mod\; 3)$, also 453 *QR* von 3;

$453 \equiv 41 \pmod{103}$;

$$\left(\frac{41}{103}\right)=\left(\frac{103}{41}\right)=\left(\frac{-20}{41}\right)=\left(\frac{20}{41}\right)=\left(\frac{5}{41}\right)\cdot\left(\frac{4}{41}\right)$$

$$\left(\frac{5}{41}\right)=\left(\frac{41}{5}\right)=\left(\frac{1}{5}\right)=1,\ \left(\frac{4}{41}\right)=1;$$

$$\left(\frac{41}{103}\right)=1.1=1, \text{ also } 453 \ QR \text{ von } 103.$$

Da nun 453 quadratischer Rest der einzelnen Factoren ist, in welche der Modul 1236, so ist es auch von diesem selbst quadratischer Rest und in der That besteht die Congruenz

$$297^2 = 88209 \equiv 453 \pmod{1236}.$$

Beispiel 4. $q = -2087$, $p = 158112 = 2^5.3^4.61$.

$$-2087 \equiv -\ 7 \pmod{32},$$
$$-2087 \equiv \ 19 \pmod{81},$$
$$-2087 \equiv -13 \pmod{61}.$$

Was nun die Zahl -7 anbetrifft, so ist sie zu Folge früherer Entwickelungen quadratischer Rest von 32; die Zahl 19 ist nach dem Modul 3 congruent mit 1 und daher ein quadratischer Rest von 3, mithin ist sie es auch von $3^4 = 81$; was endlich -13 anbetrifft, so hat man

$$\left(\frac{-13}{61}\right)=\left(\frac{13}{61}\right)=\left(\frac{61}{13}\right)=\left(\frac{9}{13}\right).$$

Aus allem zusammen ergiebt sich nun, dass -2087 ein quadratischer Rest von 158112 ist, und in der That kann man die Congruenz

$$395^2 = 156025 \equiv -2087 \pmod{158112}$$

leicht verificiren.

5) Der Satz unter 3) ist einer Erweiterung fähig, welche darum bemerkenswerth ist, weil sie zu einem Algorithmus führt, vermöge dessen der Werth des Ausdruckes $\left(\frac{q}{p}\right)$ ohne Zuziehung des Reciprocitätsgesetzes mit Leichtigkeit und in directer Weise numerisch berechnet werden kann.

Nehmen wir p und p' als zwei beliebige ungerade Zahlen an, die keinen gemeinschaftlichen Theiler haben und von denen die erste grösser als die zweite ist; dann kann man sich immer die Reihe der folgenden Divisionsgleichungen bilden:

$$(P)\quad\left\{\begin{aligned}
\frac{p}{p'} &= x + \varepsilon\frac{p''}{p'}\\
\frac{p'}{p''} &= x' + \varepsilon'\frac{p'''}{p''}\\
\frac{p''}{p'''} &= x'' + \varepsilon''\frac{p^{IV}}{p'''}\\
&\ldots\ldots\\
&\ldots\ldots\\
\frac{p^{(m-1)}}{p^{(m)}} &= x^{(m-1)} + \varepsilon^{(m-1)}\frac{p^{(m+1)}}{p^{(m)}}\\
\frac{p^{(m)}}{p^{(m+1)}} &= x^{(m)} + \varepsilon^{(m)}\frac{p^{(m+2)}}{p^{(m+1)}}\\
&\ldots\ldots\\
&\ldots\ldots\\
\frac{p^{(n-1)}}{p^{(n)}} &= x^{(n-1)} + \varepsilon^{(n-1)}\frac{p^{(n+1)}}{p^{(n)}}\\
\frac{p^{(n)}}{p^{(n+1)}} &= x^{(n)} + \varepsilon^{(n)}\frac{1}{p^{(n+1)}}
\end{aligned}\right.$$

Hier bedeuten x, x', x'', ... $x^{(n)}$ lauter solche gerade Zahlen, deren Werth den zugehörigen Brüchen auf der linken Seite am nächsten kommt und die Grössen ε, ε', ε'', ... $\varepsilon^{(n)}$ sind entweder $+1$ oder -1, je nachdem die gleichnamigen Quotientenwerthe x kleiner oder grösser sind als die zugehörigen Brüche. Die verschiedenen p werden unter dieser Voraussetzung nothwendig lauter ungerade positive Zahlen bezeichnen, die mit wechselnden Indices bis zur Grenze 1 hin abnehmen und von denen keine zwei unmittelbar auf einander folgende einen Factor mit einander gemeinschaftlich haben.

Sie sind zunächst alle ungerade Zahlen. Denn aus der ersten der Gleichungen (P) folgt

$$p = xp' + \varepsilon p''$$

und da p und p' nach Voraussetzung ungerade, x aber gerade ist, so ist $p - xp'$, d. h. $\varepsilon p''$ gleichfalls ungerade und dies ist, da ε den absoluten Werth 1 hat, nicht anders möglich als wenn p'' selbst ungerade ist. Da p' und p'' jetzt beide ungerade sind, so folgt aus der zweiten Gleichung in derselben Weise, dass auch p''' ungerade ist. Indem man so fortgeht, gelangt man zu dem Schlusse, dass sämmtliche p ungerade sind.

Hätten ferner z. B. $p^{(m+2)}$ und $p^{(m+1)}$ einen gemeinschaftlichen Theiler φ, so müsste wegen der Gleichung

$$p^{(m)} = q^{(m)}p^{(m+1)} + \varepsilon^{(m)}p^{(m+2)}$$

auch $p^{(m)}$ durch dieselbe Zahl theilbar sein und indem jetzt $p^{(m+1)}$ und $p^{(m)}$ den gemeinschaftlichen Factor φ haben, müsste φ ganz ebenso ein Factor zunächst von $p^{(m-1)}$ sein und indem man ähnliche Rückschlüsse macht, würde man zuletzt finden, dass die beiden Zahlen p und p' gegen die Voraussetzung den gemeinschaftlichen Theiler φ hätten. Also sind je zwei auf einander folgende p relative Primzahlen zu einander.

Endlich wird das letzte p, nämlich $p^{(n+2)}$ den Werth 1 haben. Denn da die p beständig abnehmen, so muss zuletzt ein p entweder gleich 0 oder gleich 1 kommen. Nun ist Ersteres nicht statthaft, weil dies voraussetzen würde, dass $p^{(n)}$ durch $p^{(n+1)}$ aufginge und mithin zwei auf einander folgende p keine relativen Primzahlen zu einander wären; mithin bleibt nur die letzte Annahme übrig.

Das Gleichungssystem (1) ist übrigens weiter nichts als die schematische Darstellung der Entwickelung des unächten Bruches $\frac{p}{p'}$ in einen Kettenbruch, dessen Zähler von der Form ± 1 und dessen Nenner lauter positive gerade Zahlen sind; in der That folgt durch eine leichte Ueberlegung:

$$\frac{p}{p'} = x + \cfrac{\varepsilon}{x' + \cfrac{\varepsilon'}{x'' + \cfrac{\varepsilon''}{x''' + \cfrac{\varepsilon'''}{x^{IV} + \dots + \cfrac{\varepsilon^{(n-1)}}{x^{(n)} + \cfrac{\varepsilon^{(n)}}{p^{(n+1)}}}}}}}.$$

Betrachten wir jetzt irgend zwei auf einander folgende Divisionsreste, etwa $p^{(m-1)}$ und $p^{(m)}$ und setzen der grösseren Kürze halber die Summe

$$E\left(\frac{p^{(m)}}{p^{(m-1)}}\right) + E\left(\frac{2p^{(m)}}{p^{(m-1)}}\right) + E\left(\frac{3p^{(m)}}{p^{(m-1)}}\right) + \dots + E\left(\frac{\frac{p^{(m-1)}-1}{2}p^{(m)}}{p^{(m-1)}}\right) = M^{(m-1)}$$

und analog

$$E\left(\frac{p^{(m+1)}}{p^{(m)}}\right) + E\left(\frac{2p^{(m+1)}}{p^{(m)}}\right) + E\left(\frac{3p^{(m+1)}}{p^{(m)}}\right) + \dots + E\left(\frac{\frac{p^{(m)}-1}{2}p^{(m+1)}}{p^{(m)}}\right) = M^{(m)}.$$

Nun ist zu Folge des Satzes unter 3), da $p^{(m)}$ und $p^{(m-1)}$ relative Primzahlen zu einander und ungerade sind,

$$\left.\begin{array}{l} E\left(\frac{p^{(m)}}{p^{(m-1)}}\right)+E\left(\frac{2p^{(m)}}{p^{(m-1)}}\right)+\ldots+E\left(\frac{\frac{p^{(m-1)}-1}{2}p^{(m)}}{p^{(m-1)}}\right) \\ +E\left(\frac{p^{(m-1)}}{p^{(m)}}\right)+E\left(\frac{2p^{(m-1)}}{p^{(m)}}\right)+\ldots+E\left(\frac{\frac{p^{(m)}-1}{2}p^{(m-1)}}{p^{(m)}}\right) \end{array}\right\} = \frac{p^{(m)}-1}{2}\cdot\frac{p^{(m-1)}-1}{2}.$$

Was die erste der beiden Horizontalreihen links betrifft, so ist sie geradezu unser $M^{(m-1)}$; die zweite betreffend folgt aus der Gleichung

$$\frac{p^{(m-1)}}{p^{(m)}} = x^{(m-1)} + \varepsilon^{(m-1)}\frac{p^{(m+1)}}{p^{(m)}}$$

die neue Gleichung

$$E\left(\frac{Ap^{(m-1)}}{p^{(m)}}\right) = E\left(Ax^{(m-1)} + \varepsilon^{(m-1)}.\frac{Ap^{(m+1)}}{p^{(m)}}\right),$$

wo A der Reihe nach die Zahlen

$$1 \quad 2 \quad 3 \quad 4 \quad \ldots\ldots \quad \frac{p^{(m)}-1}{2}$$

bedeuten möge, oder, wenn $\varepsilon^{(m-1)}$ gleich $+1$ sein sollte,

$$= Ax^{(m-1)} + \varepsilon^{(m-1)}E\left(\frac{Ap^{(m+1)}}{p^{(m)}}\right),$$

dagegen, wenn $\varepsilon^{(m-1)} = -1$ sein sollte,

$$= Ax^{(m-1)} - 1 + \varepsilon^{(m-1)}E\left(\frac{Ap^{(m+1)}}{p^{(m)}}\right).$$

Transformirt man sich in der bezeichneten Weise die sämmtlichen Glieder unserer zweiten Horizontalreihe, so erhält man $\varepsilon^{(m-1)}$ multiplicirt in die Reihe

$$E\left(\frac{p^{(m+1)}}{p^{(m)}}\right) + E\left(\frac{2p^{(m+1)}}{p^{(m)}}\right) + \ldots + E\left(\frac{\frac{p^{(m)}-1}{2}p^{(m+1)}}{p^{(m)}}\right) = M^{(m)}$$

und dazu in dem ersten der beiden genannten Fälle die Summe

$$1.x^{(m-1)} + 2x^{(m-1)} + 3x^{(m-1)} + \ldots + \frac{p^{(m)}-1}{2}x^{(m-1)} = \frac{p^{(m)}-1}{2}.\frac{p^{(m)}+1}{2}x^{(m-1)},$$

in dem zweiten dagegen dieselbe Summe, aber jedes Glied um eine Einheit verkleinert, so dass im Ganzen davon $\frac{p^{(m)}-1}{2}$ abgeht.

Setzen wir jetzt in der letzten Gleichung die für die beiden Horizontalreihen der linken Seite gefundenen Ausdrücke ein, so bekommen wir, wenn $\varepsilon^{(m-1)}$ gleich $+1$ ist,

$$M^{(m-1)}+\varepsilon^{(m-1)}M^{(m)}+\frac{p^{(m)}-1}{2}\cdot\frac{p^{(m)}+1}{2}\varkappa^{(m-1)}=\frac{p^{(m)}-1}{2}\cdot\frac{p^{(m-1)}-1}{2},$$

dagegen, wenn $\varepsilon^{(m-1)}$ gleich -1 ist,

$$M^{(m-1)}+\varepsilon^{(m-1)}M^{(m)}+\frac{p^{(m)}-1}{2}\cdot\frac{p^{(m)}+1}{2}\varkappa^{(m-1)}-\frac{p^{(m)}-1}{2}$$

$$=\frac{p^{(m)}-1}{2}\cdot\frac{p^{(m-1)}-1}{2}$$

und beide Resultate können wir zusammenfassen in der Formel:

$$M^{(m-1)}+\varepsilon^{(m-1)}M^{(m)}=\frac{p^{(m)}-1}{2}\cdot\frac{p^{(m-1)}-\varepsilon^{(m-1)}}{2}-\frac{p^{(m)}-1}{2}\cdot\frac{p^{(m)}+1}{2}\varkappa^{(m-1)}.$$

Benutzen wir die eben gefundene Recursionsformel, indem man für m der Reihe nach die Werthe

$$m=1\quad 2\quad 3\quad 4\quad 5\ \ldots\ldots\ n\quad n+1$$

einsetzt, so erhalten wir folgendes System von Formeln:

$$M+\varepsilon M'=\frac{p'-1}{2}\cdot\frac{p-\varepsilon}{2}-\frac{p'-1}{2}\cdot\frac{p'+1}{2}\varkappa$$

$$M'+\varepsilon' M''=\frac{p''-1}{2}\cdot\frac{p'-\varepsilon'}{2}-\frac{p''-1}{2}\cdot\frac{p''+1}{2}\varkappa'$$

$$M''+\varepsilon'' M'''=\frac{p'''-1}{2}\cdot\frac{p''-\varepsilon''}{2}-\frac{p'''-1}{2}\cdot\frac{p'''+1}{2}\varkappa''$$

$$M'''+\varepsilon''' M^{IV}=\frac{p^{IV}-1}{2}\cdot\frac{p'''-\varepsilon'''}{2}-\frac{p^{IV}-1}{2}\cdot\frac{p^{IV}+1}{2}\varkappa'''$$

. . . .

. . . .

$$M^{(n-1)}+\varepsilon^{(n-1)}M^{(n)}=\frac{p^{(n)}-1}{2}\cdot\frac{p^{(n-1)}-\varepsilon^{(n-1)}}{2}-\frac{p^{(n)}-1}{2}\cdot\frac{p^{(n)}+1}{2}\varkappa^{(n-1)}$$

$$M^{(n)}+\varepsilon^{(n)}M^{(n+1)}=\frac{p^{(n+1)}-1}{2}\cdot\frac{p^{(n)}-\varepsilon^{(n)}}{2}-\frac{p^{(n+1)}-1}{2}\cdot\frac{p^{(n+1)}+1}{2}\varkappa^{(n)}.$$

Die letzte unter den Grössen M, nämlich $M^{(n+1)}$ ist identisch der 0 gleich; denn es ist

$$M^{(n+1)}=E\left(\frac{p^{(n+2)}}{p^{(n+1)}}\right)+E\left(\frac{2p^{(n+2)}}{p^{(n+1)}}\right)+\ldots.$$

$$=E\left(\frac{1}{p^{(n+1)}}\right)+E\left(\frac{2}{p^{(n+1)}}\right)+\ldots.+E\left(\frac{\frac{p^{(n+1)}-1}{2}}{p^{(n+1)}}\right)$$

und jedes Glied der rechten Seite offenbar gleich 0. Wenn man jetzt die vorstehenden Recursionsformeln der Reihe nach mit

$$1\quad -\varepsilon\quad \varepsilon\varepsilon'\quad -\varepsilon\varepsilon'\varepsilon''\ \ldots\ldots\ (-1)^n\ \varepsilon\varepsilon'\varepsilon''\varepsilon'''\ \ldots\ \varepsilon^{(n-1)}$$

multiplicirt und die Producte zusammenaddirt, so hebt sich links alles bis auf das erste Glied oben und das letzte Glied unten, welches für sich selber schon verschwindet, und es resultirt daher:

$$
\begin{aligned}
M = \quad & \frac{p'-1}{2}\cdot\frac{p-\varepsilon}{2} - \frac{p'-1}{2}\cdot\frac{p'+1}{2}\,x \\
-\varepsilon\, & \frac{p''-1}{2}\cdot\frac{p'-\varepsilon'}{2} + \varepsilon\,\frac{p''-1}{2}\cdot\frac{p''+1}{2}\,x' \\
+\varepsilon\varepsilon'\, & \frac{p'''-1}{2}\cdot\frac{p''-\varepsilon''}{2} - \varepsilon\varepsilon'\,\frac{p'''-1}{2}\cdot\frac{p'''+1}{2}\,x'' \\
-\varepsilon\varepsilon'\varepsilon''\, & \frac{p^{IV}-1}{2}\cdot\frac{p'''-\varepsilon'''}{2} + \varepsilon\varepsilon'\varepsilon''\,\frac{p^{IV}-1}{2}\cdot\frac{p^{IV}+1}{2}\,x''' \\
& \cdots\cdots\cdots\cdots \\
& \cdots\cdots\cdots\cdots \\
(-1)^{n-1}\varepsilon\varepsilon'\varepsilon''\ldots\varepsilon^{(n-2)}\, & \frac{p^{(n)}-1}{2}\cdot\frac{p^{(n-1)}-\varepsilon^{(n-1)}}{2} - (-1)^{n-1}\varepsilon\varepsilon'\ldots\varepsilon^{(n-2)}\frac{p^{(n)}-1}{2} \\
& \qquad\cdot\frac{p^{(n)}+1}{2}\,x^{(n-1)} \\
(-1)^{n}\varepsilon\varepsilon'\ldots\varepsilon^{(n-1)}\, & \frac{p^{(n+1)}-1}{2}\cdot\frac{p^{(n)}-\varepsilon^{(n)}}{2} - (-1)^{n}\varepsilon\varepsilon'\ldots\varepsilon^{(n-1)}\frac{p^{(n+1)}+1}{2} \\
& \qquad\cdot\frac{p^{(n+1)}+1}{2}\,x^{(n)}.
\end{aligned}
$$

Nehmen wir jetzt p speciell als Primzahl an, $q = p'$ dagegen als eine beliebige oder zusammengesetzte ungerade Zahl kleiner als p, so folgt aus den beiden Sätzen unter 1) und 2), dass, je nachdem M gerade oder ungerade ist, der Ausdruck $\left(\frac{q}{p}\right) = +1$ oder gleich -1, d. h. mit anderen Worten q quadratischer Rest oder Nichtrest von p wird. Demgemäss ist für unseren Zweck blos die Untersuchung von M darauf hin, ob es gerade oder ungerade sei, nothwendig und wir können daher in dem Ausdrucke rechts alle Multipla von 2 weglassen, d. h. da die Grössen $x, x', x'', \ldots\ldots$ alle gerade Zahlen sind, zunächst die sämmtlichen Glieder in zweiter Stelle. Ferner können wir auch allen Gliedern ohne Ausnahme das Vorzeichen $+$ geben, d. h. die Producte der $\varepsilon, \varepsilon', \varepsilon'', \ldots$ vernachlässigen; denn wenn etwa eines das Vorzeichen -1 geben sollte, so kann man immer durch Addition des doppelten Gliedes das Vorzeichen in $+$ transformiren. Dadurch bekommen wir

$$M \equiv \frac{p'-1}{2}\,\frac{p-\varepsilon}{2}+\frac{p''-1}{2}\,\frac{p'-\varepsilon'}{2}+\frac{p'''-1}{2}\,\frac{p''-\varepsilon''}{2}+\frac{p^{IV}-1}{2}\,\frac{p'''-\varepsilon'''}{2}$$
$$+\ldots\ldots+\frac{p^{(n+1)}-1}{2}\,\frac{p^{(n)}-\varepsilon^{(n)}}{2}\ (mod\ 2).$$

Da die Zahlen p, p', p'', ... alle ungerade sind, so ist jedes Glied der rechten Seite entweder eine gerade oder eine ungerade Zahl und von der Anzahl der letzteren Glieder wird die Beschaffenheit des M abhängen. Ist die Anzahl der Glieder, welche eine ungerade Zahl geben, eine ungerade, so wird M nothwendig auch ungerade sein; in allen anderen Fällen ist M gerade.

Ob irgend ein specielles Glied, etwa $\frac{p'''-1}{2}\cdot\frac{p''-\varepsilon''}{2}$ gerade oder ungerade ist, kann man leicht entscheiden; es ist nämlich gerade, wenn entweder beide Factoren $p'''-1$ und $p''-\varepsilon''$, oder wenigstens eine von ihnen die Form $4n$ hat; dagegen ungerade, d. h. nach dem Modul 2 der Einheit congruent, wenn beide genannten Factoren von der Form $4n+2$ sind. Die Bildung dieser Factoren ist sehr einfach, wenn man bemerkt, dass die darin vorkommenden Grössen p''', p'', ε'' alle durch ein einziges der in (P) aufgeführten Divisionsexempel erhalten werden. Der erste Factor ist nämlich der Divisor vermindert um die Einheit, der zweite Factor der Dividendus vermindert um das zugehörige ε, d. h. wenn ε gleich $+1$ sein sollte, vermindert um 1, dagegen, wenn ε gleich -1 sein sollte, vermehrt um 1. Schreibt man sich demgemäss neben jedes Divisionsexempel entweder 1 oder nichts, je nachdem entweder beide Factoren durch 2 dividirt ungerade Zahlen geben oder wenigstens einer von ihnen gerade ausfällt, so ist $\left(\frac{q}{p}\right)=\left(\frac{p'}{p}\right)$ gleich $+1$ oder gleich -1, je nachdem die Anzahl dieser Einsen gerade oder ungerade ist. Das Detail der Anwendung möge aus folgenden Beispielen entnommen werden:

Beispiel 1.

$$\left(\frac{601}{1013}\right)=-1.$$

601 | 1013 | 2 $\qquad \frac{601-1}{2}\cdot\frac{1013+1}{2}$ gerade

1202

—189 | 601 | 4 $\qquad \frac{189-1}{2}\cdot\frac{601+1}{2}$ gerade

756

—155 | 189 | 2 $\qquad \frac{155-1}{2}\cdot\frac{189+1}{2}$ ungerade also $\equiv$ 1

310

—121 | 155 | 2 $\qquad \frac{121-1}{2}\cdot\frac{155+1}{2}$ gerade

242

—87 | 121 | 2 $\qquad$ 1

174

—53 | 87 | 2

106

—19 | 53 | 2 $\qquad \frac{19-1}{2}\cdot\frac{53-1}{2}$ gerade

38

+15 | 19 | 2

30

—11 | 15 | 2

22

—7 | 11 | 2

14

—3 | 7 | 2 $\qquad \frac{1}{3}$

6

+1

Beispiel 2.

$$\left(\frac{-402}{929}\right) = (-402)^{464} = (402)^{464} = \left(\frac{402}{929}\right) = \left(\frac{2}{929}\right)\cdot\left(\frac{201}{929}\right);$$

$$\left(\frac{2}{929}\right) = \frac{2}{(8.116+1)} = 1, \quad \left(\frac{201}{929}\right) = 1;$$

$$\left(\frac{-402}{929}\right) = 1.$$

201 | 929 | 4

804

125 | 201 | 2

250

—49 | 125 | 2

98

27 | 49 | 2 $\qquad$ 1

54

—5 | 127 | 6

30

—3 | 5 | 2 $\qquad \frac{1}{2}$

6

—1

Beispiel 3.

$$\left(\frac{343}{773}\right) = -1$$

$$\begin{array}{l}
343\,|\,773\,|\,2 \\
\quad\;\; \underline{686} \\
\quad\;\; 87\,|\,343\,|\,4 \\
\qquad\quad \underline{348} \\
\qquad\quad -5\,|\,87\,|\,18 \\
\qquad\qquad\;\; \underline{90} \\
\qquad\qquad -3\,|\,5\,|\,2 \qquad \frac{1}{1} \\
\qquad\qquad\quad\;\; \underline{6} \\
\qquad\qquad\quad -1
\end{array}$$

Ein ähnlicher, wenn auch etwas weitläufigerer Algorithmus, der von Eisenstein herrührt, findet sich in Crell's Journal Bd. 27 p. 317 und 318. Indessen ist der daselbst mitgetheilte Beweis ungenügend, da er das Reciprocitätsgesetz als gültig voraussetzt, selbst wenn die beiden Zahlen q und p, die in den Ausdruck $\left(\frac{q}{p}\right)$ hineingehen, nicht beide Primzahlen sind, eine Voraussetzung, die durchaus nicht unter allen Umständen erfüllt zu werden braucht.

Um dies durch ein Beispiel zu belegen, bemerken wir, dass die Congruenz

$$7^2 = 49 \equiv 15 \ (mod\ 17)$$

besteht und demgemäss

$$\left(\frac{15}{17}\right) = 1$$

sein muss. Zu Folge des Reciprocitätsgesetzes würde hieraus folgen:

$$1 = \left(\frac{15}{17}\right) = \left(\frac{17}{15}\right) \equiv 17^7 \ (mod\ 15).$$

Nun ist aber in Wahrheit

$$17^7 = (15+2)^7 \equiv 2^7 = 128 \equiv 8 \ (mod\ 15)$$

und mithin liefert die Anwendung des genannten Gesetzes ein offenbar falsches Resultat.

Vermittelst des Reciprocitätsgesetzes, ferner vermittelst der Sätze in §. 15, sowie endlich vermittelst der Sätze in §. 16, welche die Zahlen —1 und 2 in ihrer Eigenschaft Reste oder Nichtreste einer gegebenen Primzahl zu sein betreffen, ist man unter allen Umständen im Stande die Entscheidung zu treffen, ob eine sei es einfache oder zusammenge-

setzte Zahl q quadratischer Rest oder Nichtrest irgend eines beliebigen Moduls P sei. Indessen ist diese Untersuchung von zu specieller Natur, als dass sie uns weiter beschäftigen könnte und wir wenden uns daher wieder der Untersuchung solcher allgemeinen Formen des Moduls p (die wir fortwährend als eine ungerade Primzahl voraussetzen) zu, denen eine specielle Zahl q als Rest oder Nichtrest entspricht.

§. 18.

Von den linären Formen der Primzahl p, welche Divisoren oder Nicht-Divisoren des Ausdruckes $x^2 - q$ sind.

1) Untersuchung der Zahlen 7 und 11.

Zu Folge des Reciprocitätsgesetzes hat man, da 7 von der Form $4n - 1$ ist,

$$\left(\frac{7}{p}\right) = \pm\left(\frac{p}{7}\right),$$

je nachdem die Primzahl p von der Form $4n+1$ oder $4n-1$ ist. Nun sind die verschiedenen Formen, deren irgend eine Primzahl in Bezug auf den Modul 7 fähig ist,

$$7n+1 \quad 7n+2 \quad 7n+3 \quad 7n-3 \quad 7n-2 \quad 7n-1$$

und darunter sind Reste von 7 die Formen

$$7n+1 \quad 7n+2 \quad 7n-3$$

und Nichtreste die Formen

$$7n+3 \quad 7n-2 \quad 7n-1.$$

Wählen wir irgend eine specielle unter den vorstehenden Formen und bezeichnen dieselbe durch

$$7n \pm r,$$

so kommt es darauf an, diejenigen unter den Primzahlen dieser Form, welche zugleich von der Form $4n+1$ sind, von denjenigen zu unterscheiden, welche zugleich von der Form $4n-1$ sind. Das ist aber nichts anderes als die Aufgabe diejenigen beiden Zahlformen zu bestimmen, welche durch 7 dividirt den Rest r und durch 4 dividirt entweder den Rest $+1$ oder -1 lassen. Um diese Bestimmung zu leisten stellen wir in Uebereinstimmung mit §. 8, 1) die Hülfscongruenzen

$$4m \equiv 1 \ (mod\ 7)$$
$$7m' \equiv 1 \ (mod\ 4)$$

auf, durch deren Auflösung in den kleinsten Zahlen wir

$$m = 2,\ 4m = 8$$
$$m' = -1,\ 7m' = -7$$

erhalten und bilden uns die beiden allgemeinen Ausdrücke

$$8r - 7,$$
$$8r + 7;$$

alsdann bekommen wir, indem wir für r nach einander die ihm zukommenden speciellen Zahlenwerthe

$$+1 \quad +2 \quad -3 \quad +3 \quad -2 \quad -1$$

einsetzen und jedesmal die kleinsten Zahlen nehmen:

$$p = \begin{cases} 8r - 7 \equiv \quad 1 \quad 9 \quad -3 \quad -11 \quad 5 \quad 13 \\ 8r + 7 \equiv -13 \quad -5 \quad 11 \quad 3 \quad -9 \quad -1 \end{cases} (mod\ 28).$$

Demgemäss sind folgende 6 Formen der Primzahl p Reste von 7:

$$28n + 1 \quad 28n + 9 \quad 28n - 3$$
$$28n - 13 \quad 28n - 5 \quad 28n + 11$$

und folgende 6 Formen der Primzahl p Nichtreste von 7:

$$28n - 11 \quad 28n + 5 \quad 28n + 13$$
$$28n + 3 \quad 28n - 9 \quad 28n - 1.$$

Was nun die jedesmaligen drei oberen Formen betrifft, so sind sie dasselbe in Bezug auf p, was sie in Bezug auf 7 sind; die jedesmaligen drei unteren dagegen sind in Bezug auf p gerade das Entgegengesetzte von demjenigen, was sie in Bezug auf 7 sind. Also ist 7 ein quadratischer Rest von folgenden Formen der Primzahl p:

$$28n + 1 \quad 28n + 9 \quad 28n - 3 \quad 28n + 3 \quad 28n - 9 \quad 28n - 1$$

und quadratischer Nichtrest von folgenden Formen der Primzahl p:

$$28n - 13 \quad 28n - 5 \quad 28n + 11 \quad 28n - 11 \quad 28n + 5 \quad 28n + 13.$$

Nehmen wir eine ähnliche Untersuchung rücksichtlich der Zahl 11 vor, so haben zunächst die Reste von 11 alle eine der Formen

$$11n + 1 \quad 11n + 3 \quad 11n + 4 \quad 11n + 5 \quad 11n - 2$$

und darunter sind diejenigen, welche zugleich die Form $4n + 1$ haben:

$$44n + 1 \quad 44n - 19 \quad 44n - 7 \quad 44n + 5 \quad 44n + 9$$

und diejenigen, welche zugleich die Form $4n - 1$ haben:

$$44n - 21 \quad 44n + 3 \quad 44n + 15 \quad 44n - 17 \quad 44n - 13.$$

Ferner die Nichtreste von 11 sind nothwendig von einer der Formen:

$11n+2 \quad 11n-5 \quad 11n-4 \quad 11n-3 \quad 11n-1$

und darunter sind diejenigen, welche zugleich von der Form $4n+1$ sind:

$44n+13 \quad 44n+17 \quad 44n-15 \quad 44n-3 \quad 44n-21$

und diejenigen, welche von der Form $4n-1$ sind:

$44n-9 \quad 44n-5 \quad 44n+7 \quad 44n+19 \quad 44n-1.$

Die Anwendung des Satzes der Reciprocität ergiebt nun unmittelbar, dass für alle Primzahlen der Form:

$44n+1 \quad 44n-19 \quad 44n-7 \quad 44n+5 \quad 44n+9$

$44n-9 \quad 44n-5 \quad 44n+7 \quad 44n-5 \quad 44n-9$

die Zahl 11 ein Rest ist, und für alle Primzahlen der Form

$44n-21 \quad 44n+3 \quad 44n+15 \quad 44n-17 \quad 44n-13$

$44n+13 \quad 44n+17 \quad 44n-15 \quad 44n+17 \quad 44n+13$

ein Nichtrest.

Wenn wir eine beliebige solche Form herausnehmen, für welche 11 ein Rest ist, z. B. die Form $44n-9$, so heisst dies doch nichts anderes, als die Congruenz

$$x^2 \equiv 11 \ (mod\ 44n-9)$$

ist immer möglich, oder mit anderen Worten, es lassen sich immer zwei solche Werthe von x bestimmen, dass irgend eine beliebige Primzahl von der Form $44n-9$ ein Divisor des Ausdruckes x^2-11 werde. In ähnlichem Sinne sind die (in Bezug auf n) linearen Formen, welche die Fähigkeit haben Divisoren des Ausdruckes

$$x^2-7$$

werden zu können, folgende sechs:

$28n+1 \quad 28n+9 \quad 28n-3 \quad 28n+3 \quad 28n-9 \quad 28n-1$

und alle Primzahlen, welche eine davon verschiedene Form, nämlich eine der Formen

$28n-13 \quad 28n-5 \quad 28n+11 \quad 28n-11 \quad 28n+5 \quad 28n+13$

haben, können überhaupt niemals Divisoren des Ausdruckes x^2-7 werden, d. h. es existirt kein endliches bestimmtes x, für welches diese Differenz ein Multiplum irgend einer solchen Primzahl werden könnte. Dies ist die gewöhnliche Form, in welcher die Theorie der quadratischen Reste und Nichtreste in die Anwendung hineinspielt. Verallgemeinern wir die eben angestellte Betrachtung, so kommen wir zu folgendem Theoreme:

2) Wenn p und q zwei ungerade Primzahlen bezeichnen, so existiren immer $q-1$ nach dem Modul $4q$ von einander verschiedene lineäre Formen der Primzahl p, welche Divisoren des Ausdruckes

$$x^2-q$$

werden können und ebensoviele lineäre Formen der Primzahl p bleiben übrig, welche Nicht-Divisoren des genannten Ausdruckes sind. Mit diesen $2(q-1)$ Formen sind alle Formen erschöpft, deren irgend eine Primzahl nach dem Modul $4q$ überhaupt fähig ist, und zugleich ordnen sie sich alle der allgemeinen Form

$$4qn+R$$

unter, wo n eine beliebige ganze Zahl und R eine Zahl kleiner als q und relative Primzahl zu q bezeichnet.

Zunächst sieht man ohne Weiteres ein, dass die Anzahl der R gleich $S'''(4q)=2(q-1)$ ist und dass keine Primzahl p existirt, welche von einer anderen Form als einer der genannten sein kann. Um diese Formen alle zu erhalten bilde man sich alle nur möglichen nach dem Modul q von einander verschiedenen Formen der Primzahl p, nämlich

$$qn+\frac{q-1}{2},\ qn+\frac{q-3}{2},\ \ldots.\ 2,\ 1,\ -1,\ -2,\ \ldots.\ qn-\frac{q-3}{2},\ qn-\frac{q-1}{2}$$

und bestimme sich darauf rücksichtlich jeder dieser Formen zwei Partialformen, von denen die eine alle Zahlen umfasst, die nach dem Modul 4 den Rest 1 und die andere alle Zahlen, die nach dem Modul 4 den Rest -1 lassen. Auf diese Weise möge allgemein irgend eine

$$qn+r$$

der beiden vorhergehenden Formen in die beiden Partialformen

$$4qn+r',\ 4qn+r''$$

zerfallen: dann sind alle die den verschiedenen Werthen von r entsprechenden r' und r'' (nach dem Modul $4q$) von einander verschieden und relative Primzahlen zu $4q$. Um dieses zu beweisen, denken wir uns unter r irgend einen beliebigen speciellen Zahlenwerth und nehmen an, ϱ wäre ein anderer specieller davon (nach dem Modul q) verschiedener Zahlenwerth; dann werden zwischen den r', r'', ϱ', ϱ'' folgende Congruenzen eintreten:

$$r' \equiv r \pmod q;\ r'' \equiv \ \ r \pmod q$$
$$r' \equiv 1 \pmod 4;\ r'' \equiv -1 \pmod 4$$

und

$$\varrho' \equiv \varrho \pmod q;\ \varrho'' \equiv \ \ \varrho \pmod q$$
$$\varrho' \equiv 1 \pmod 4;\ \varrho'' \equiv \ \ 1 \pmod 4.$$

Hier können nun zunächst keine r und ϱ mit gleicher Anzahl von Strichen einander gleich sein; denn daraus würde folgen

$$r \equiv \varrho \pmod q$$

gegen die Voraussetzung, nach der r und ϱ von einander verschiedene Zahlen (absolut genommen) > 0 und $< \frac{q-1}{2}$ sind; ebensowenig können 2 solcher r und ϱ mit ungleicher Anzahl von Strichen gleich sein, denn daraus würde die gleichfalls widersinnige Congruenz

$$1 \equiv -1 \pmod 4$$

folgen. Endlich sind auch r', ϱ', r'', ϱ'' alle relative Primzahlen zu $4q$. Denn wäre z. B. r' keine relative Primzahl zu q, so wäre die Congruenz

$$r' \equiv r \pmod q$$

widersinnig, und wäre r' keine relative Primzahl auch zu 4, so wäre die Congruenz

$$r' \equiv 1 \pmod 4$$

gleichfalls sinnlos. Da also r' sowohl zu 4, wie zu q relative Primzahl ist und 4 und q gleichfalls keinen gemeinschaftlichen Factor haben, so ist r' auch relative Primzahl zu dem Produkte $4q$.

Die Anzahl der Partialformen, die aus der beschriebenen Zerfällung hervorgehen, ist offenbar gleich $2(q-1)$ und zwar sind die Hälfte darunter der allgemeinen Form $4n+1$ unterworfen, während die andere Hälfte sich der allgemeinen Form $4n-1$ unterordnet; zugleich ist dieselbe gleich der Anzahl der relativen Primzahlen zu $4q$, wie es sein muss.

Bemerkt man nun, dass im Ganzen $\frac{q-1}{2}$ nach dem Modul q verschiedene Formen von p existiren, welche Reste von q sind, und eben so viele, welche Nichtreste sind, so bekommt man folgende 4 Klassen, in welchen alle nur überhaupt existirenden Primzahlen inbegriffen sind:

a) $\frac{q-1}{2}$ verschiedene Formen von p, welche Reste von q sind und sich der allgemeinen Form $4n+1$ unterordnen.

b) $\frac{q-1}{2}$ verschiedene Formen von p, welche Reste von q sind und sich der allgemeinen Form $4n-1$ unterordnen.

c) $\frac{q-1}{2}$ verschiedene Formen von p, welche Nichtreste von q sind und sich der allgemeinen Form $4n+1$ unterordnen.

d) $\frac{q-1}{2}$ verschiedene Formen von p, welche Nichtreste von q sind und sich der allgemeinen Form $4n-1$ unterordnen.

Wenn nun q von der Form $4n+1$ ist, so stellen nach dem Gesetze der Reciprocität die Gruppen a) und b) alle nur möglichen Modul p dar, von welchen q Rest ist, und die Gruppen c) und d) sind alle nur möglichen Modul, von welchen q Nichtrest ist; oder anders ausgedrückt, die in den Gruppen a) und b) vorkommenden Formen von p sind alle Divisoren von x^2-q, dagegen die in den Gruppen c) und d) vorkommenden Formen von p sind Nicht-Divisoren von x^2-q. Wenn dagegen q von der Form $4n-1$ ist, so stellen die in den Gruppen a) und d) vorkommenden Zahlen alle nur möglichen Divisoren von x^2-q dar und die in den Gruppen b) und c) vorkommenden Zahlen alle nur möglichen Nicht-Divisoren. Wir bekommen also in beiden Fällen zusammen $(q-1)$ Divisoren und ebensoviele Nicht-Divisoren.

Wir fügen noch hinzu, dass es bei Bestimmung dieser Divisoren vollkommen gleichgültig ist, ob man die in den zugehörigen Ausdrücken vorkommenden relativen Primzahlen zu $4q$ alle positiv und zwischen den Grenzen 0 und $4q$ hat, oder ob man an Stelle derjenigen, welche grösser sind als $2q$, ihre kleinsten Reste setzt, welche letztern sämmtlich die, negativ genommenen, relativen Primzahlen zu $4q$ unterhalb der Grenze $2q$ sein werden.

3) Gehen wir jetzt weiter und suchen unter der Voraussetzung eines zusammengesetzten q die Formen derjenigen Primzahlen, welche Divisoren oder Nicht-Divisoren des Ausdruckes x^2-q sind; so ist zunächst ersichtlich, dass man alle in q etwa enthaltenen quadratischen Factoren ohne Weiteres ausscheiden kann. Dann sei $q=rs^2$, so ist die Bedingung dafür, dass q quadratischer Rest von p sei,

$$\left(\frac{q}{p}\right)=\left(\frac{rs^2}{p}\right)=\left(\frac{r}{p}\right)\cdot\left(\frac{s^2}{p}\right)=1$$

und da bekanntlich für jeden beliebigen Werth von s (der kein Vielfaches von p ist) die Relation

$$\left(\frac{s^2}{p}\right) \equiv s^{2\cdot\frac{p-1}{2}} = s^{p-1} \equiv 1$$

besteht, so ist offenbar q quadratischer Rest oder Nichtrest, je nachdem es r ist. Hiernach können wir q als ein Product von m unter einander verschiedenen Primfactoren von der Form

$$q = \alpha\beta\gamma \;\ldots\ldots\; \lambda\mu\nu \;\ldots\ldots$$

betrachten, wo α, β, γ .... sämmtlich Primfactoren der Form $4n+1$, dagegen λ, μ, ν .... sämmtlich Primfactoren der Form $4n-1$ bezeichnen.

Nun hat man

$$\left(\frac{q}{p}\right) = \left(\frac{\alpha}{p}\right)\cdot\left(\frac{\beta}{p}\right)\cdot\left(\frac{\gamma}{p}\right) \ldots\ldots \left(\frac{\lambda}{p}\right)\cdot\left(\frac{\mu}{p}\right)\cdot\left(\frac{\nu}{p}\right)$$

und es wird q ein quadratischer Rest von p sein, wenn die Anzahl der Factoren rechts, welche mit -1 congruent werden, entweder gleich 0 oder eine gerade Zahl ist, dagegen ein quadratischer Nichtrest, wenn diese Anzahl ungerade ausfällt. Beides zusammengenommen erschöpft die sämmtlichen Variationen mit Wiederholungen zur $m$ten Klasse, welche zwischen den Vorzeichen + und -1 möglich sind und deren Anzahl gleich 2^m ist. Die Hälfte dieser Variationen entspricht einem q, welches Rest von p, und die andere einem q, welches Nichtrest von p ist. Denn durch eine leichte Induction erhellt, dass, wie auch m beschaffen sein möge, die Anzahl der Variationen, in denen eine ungerade Anzahl von -1 vorkommt, gleich der Anzahl derjenigen Variationen ist, in denen die Minus entweder ganz fehlen oder doch nur in gerader Anzahl vorkommen.

Nun kann p entweder von der Form $4n+1$ oder von der Form $4n-1$ sein. Zu Folge der genannten Schlussfolgen bekommen wir in jedem von diesen beiden Fällen 2^m der bezeichneten Variationen, von denen die Hälfte einem Rest von q, die andere Hälfte einem Nichtrest von q entspricht, mithin sind es im Ganzen 2.2^m solcher Variationen. Die Anwendung des Gesetzes der Reciprocität giebt im ersten Falle

$$\left(\frac{q}{p}\right) = \left(\frac{p}{\alpha}\right)\cdot\left(\frac{p}{\beta}\right)\cdot\left(\frac{p}{\gamma}\right) \ldots\ldots \left(\frac{p}{\lambda}\right)\cdot \left(\frac{p}{\mu}\right)\cdot \left(\frac{p}{\nu}\right)\ldots\ldots$$

und im zweiten Falle

$$\left(\frac{q}{p}\right) = \left(\frac{p}{\alpha}\right)\cdot\left(\frac{p}{\beta}\right)\cdot\left(\frac{p}{\gamma}\right) \ldots\ldots -\left(\frac{p}{\lambda}\right)\cdot -\left(\frac{p}{\mu}\right)\cdot -\left(\frac{p}{\nu}\right)\ldots\ldots$$

und dies vorausgesetzt kann man leicht zeigen, dass jede specielle Variation, der eine bestimmte Folge der Vorzeichen + und — entspricht, im Ganzen

$$\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdots\cdots\frac{\lambda-1}{2}\cdot\frac{\mu-1}{2}\cdot\frac{\nu-1}{2}\cdots\cdots$$

Formen von p liefert, welche entweder die Zahl q alle zugleich zum Reste oder alle zugleich zum Nichtreste haben, nämlich ersteres, wenn die Minus in gerader Anzahl, letzteres, wenn die Minus in ungerader Anzahl hineingehen.

In der That mögen den Factoren der betrachteten Variation beispielsweise folgende Werthe entsprechen:

$$\left(\frac{p}{\alpha}\right)\equiv p^{\frac{\alpha-1}{2}}\equiv +1 \ (mod\ \alpha)$$

$$\left(\frac{p}{\beta}\right)\equiv p^{\frac{\beta-1}{2}}\equiv -1 \ (mod\ \beta)$$

$$\left(\frac{p}{\gamma}\right)\equiv p^{\frac{\gamma-1}{2}}\equiv -1 \ (mod\ \gamma)$$

$$\cdots\cdots$$

$$\cdots\cdots$$

$$\left(\frac{p}{\lambda}\right)\equiv p^{\frac{\lambda-1}{2}}\equiv -1 \ (mod\ \lambda)$$

$$\left(\frac{p}{\mu}\right)\equiv p^{\frac{\mu-1}{2}}\equiv +1 \ (mod\ \mu)$$

$$\left(\frac{p}{\nu}\right)\equiv p^{\frac{\nu-1}{2}}\equiv -1 \ (mod\ \nu)$$

$$\cdots\cdots$$

$$\cdots\cdots$$

so erhellt unmittelbar, dass die vorstehenden Congruenzen soviele nach dem Modul

$$q=\alpha\beta\gamma\ \ldots\ldots\ \lambda\mu\nu\ \ldots\ldots$$

von einander verschiedene Formen von p liefern, als Combinationen zwischen ihren verschiedenen Lösungen möglich sind, d.h. die Anzahl der resultirenden Formen ist

$$\frac{\alpha-1}{2}\cdot\frac{\beta-1}{2}\cdot\frac{\gamma-1}{2}\cdots\cdots\frac{\lambda-1}{2}\cdot\frac{\mu-1}{2}\cdot\frac{\nu-1}{2}\cdots\cdots$$

Da das Gleiche von allen anderen Variationen gilt, welche irgend welchen anderen Folgen von Vorzeichen entsprechen, so erhalten wir im Ganzen 2.2^m Klassen von Formen der Primzahl p, deren jede die eben genannte Anzahl von einander verschiedener Formen umfasst. Von diesen 2.2^m Klassen sind näher 2^m von der Form $4n+1$, so dass sie durch Combination der beiden Eintheilungsmodul auf die Form

$$4qn+\alpha,\ \alpha \equiv 1\ (mod\ 4)$$

kommen, wo α irgend eine relative Primzahl zu $4q$ bezeichnet; die eine Hälfte darunter besteht aus lauter Divisoren, die andere Hälfte aus lauter Nicht-Divisoren des Ausdruckes x^2-q. Die übrig bleibenden 2^m Klassen umfassen gleichfalls zur Hälfte Divisoren und zur Hälfte Nicht-Divisoren von x^2-q, im Uebrigen aber lauter Zahlen der Form $4n-1$, so dass die schliesslich resultirenden Formen durch Combination der Eintheilungsmodul 4 und q auf die Gestalt

$$4qn+\beta,\ \beta \equiv -1\ (mod\ 4)$$

kommen, wo β wiederum irgend welche bestimmte relative Primzahlen zu $4q$ bezeichnet.

Fassen wir alles Bisherige zusammen, so haben wir überhaupt in sämmtlichen Klassen

$$2.2^m.\frac{\alpha-1}{2}.\frac{\beta-1}{2}.\frac{\gamma-1}{2}\ldots\ldots\frac{\lambda-1}{2}.\frac{\mu-1}{2}.\frac{\nu-1}{2}\ldots\ldots$$

von einander verschiedene Formen der Primzahl p, die nach dem Modul $4q$ alle von einander verschieden ausfallen und in der That ist dieses die Anzahl der nach dem Eintheilungsmodul $4q$ überhaupt möglichen Formen; denn der letztgenannte Ausdruck ist offenbar, wenn man die in der Potenz 2^m enthaltenen Factoren 2 gegen die sämmtlichen in den Nennern vorkommenden Factoren 2 aufhebt,

$$= 2(\alpha-1)(\beta-1)(\gamma-1)\ldots.(\lambda-1)(\mu-1)(\nu-1)\ldots.$$
$$= S'''4q.$$

Dieser letzte Ausdruck giebt aber die Zahl der möglichen Formen von p an; denn, damit

$$p = 4qn+\gamma$$

eine Primzahl sein könne, darf γ keinen Theiler mit $4q$ gemeinschaftlich besitzen und muss mithin als eine Zahl kleiner als $4q$ und relative Primzahl zu $4q$ angenommen werden.

Wir haben bei dieser Betrachtung einen speciellen Fall ausser Acht gelassen, nämlich den, wenn q zu einem seiner Factoren die einzige gerade Primzahl 2 hat. Sei also

$$q' = 2q;$$

dann ist

$$\left(\frac{q'}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{q}{p}\right)$$

und 2 quadratischer Rest für die Formen

$$8n+1, \; 8n-1;$$

quadratischer Nichtrest für die Formen

$$8n+3, \; 8n-3.$$

Indem nun q ein Rest von $\frac{1}{4}.2^m$ Klassen von Formen der Primzahl p ist, welche sich der allgemeinen Form $4n+1$ unterordnen, lassen sich dieselben in 2 Abtheilungen bringen, die eine Hälfte von der Form $8n+1$ und lauter Divisoren von x^2-q', die andere Hälfte von der Form $8n-3$ und lauter Nicht-Divisoren von x^2-q'. Ebenso verhält es sich mit den $\frac{1}{4}.2^m$ Formenklassen der Primzahl p, welche q zum Nichtreste haben und von der Form $4n+1$ sind. Was ferner die $\frac{1}{4}.2^m$ Formenklassen der p betrifft, welche q zum Reste und die Form $4n-1$ haben, sowie die gleich grosse Anzahl von Klassen der p, welche q zum Nichtreste und die nämliche Form $4n-1$ haben, so erhalten wir in beiden Fällen die eine Hälfte von der Form $8n-1$ und aus lauter Divisoren bestehend, die andere Hälfte von der Form $8n+3$ und aus lauter Nicht-Divisoren bestehend.

Schliesslich kommen also 2^{m+1} nach dem Modul $8q$ von einander verschiedene Klassen von Formen der Primzahl p heraus, welche Divisoren, und ebensoviele, welche Nicht-Divisoren des Ausdruckes x^2-q' sind.

Es wird zur Veranschaulichung der vorhergehenden Erörterungen nicht unpassend sein ein vollständig durchgerechnetes Beispiel folgen zu lassen. Stellen wir uns also die Aufgabe: D i e P r i m z a h l e n z u s u c h e n, w e l c h e D i v i s o r e n v o n x^2+105 sind. Es ist hiernach

$$q = -3.5.7, \; m = 3, \; 2^m = 8;$$

mithin giebt es 8 Klassen von Formen des Divisors p, darunter sind 4, die sich der Form $4n+1$, und 4, die sich der Form $4n-1$ unterordnen. Jede Klasse besteht aus $\frac{3-1}{2} \cdot \frac{5-1}{2} \cdot \frac{7-1}{2} = 6$ von einander verschiedenen Formen. Wir unterscheiden hiernach 2 Hauptabtheilungen:

I. Die Primzahl p ist von der Form $4n+1$.

Es wird alsdann

$$\left(\frac{-3}{p}\right)=(-3)^{\frac{p-1}{2}}=3^{\frac{p-1}{2}}=\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right);$$

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right),\ \left(\frac{7}{p}\right)=\left(\frac{p}{7}\right),$$

und man bekommt mithin

$$\left(\frac{-105}{p}\right)=\left(\frac{p}{3}\right)\cdot\left(\frac{p}{5}\right)\cdot\left(\frac{p}{7}\right).$$

Die verschiedenen Variationen der Vorzeichen rechts, welche + geben und —105 als einen Rest von p bestimmen, sind folgende:

$$\begin{array}{llll}
(1) & \left(\frac{p}{3}\right)=+1; & \left(\frac{p}{5}\right)=+1; & \left(\frac{p}{7}\right)=+1; \\
(2) & \quad =+1 & \quad =-1 & \quad =-1 \\
(3) & \quad =-1 & \quad =+1 & \quad =-1 \\
(4) & \quad =-1 & \quad =-1 & \quad =+1.
\end{array}$$

Jede dieser Variationen bestimmt eine Restklasse, welche aus 6 verschiedenen Formen besteht. Um diese Formen zu erhalten bemerke man, dass die Primzahlen p, welche quadratische Reste von 3, 5, 7 sind, respective die folgende Form haben müssen:

$$p=3n+1;$$
$$p=5n+1,\ 5n+4;$$
$$p=7n+1,\ 7n+2,\ 7n+4;$$

sowie dass die Primzahlen p, welche quadratische Nichtreste der genannten Modul sind, sich mit Nothwendigkeit bezüglich den folgenden Formen unterordnen:

$$p=3n+2;$$
$$p=5n+2,\ 5n+3;$$
$$p=7n+3,\ 7n+5,\ 7n+6.$$

Hiernach entsprechen den verschiedenen Klassen alle möglichen Combinationen, welches bezugsweise jedes der 4 folgenden Systeme von Congruenzen gestattet:

$$(1)\ \begin{cases} p\equiv 1\ (mod\ 3) \\ p\equiv 1,\ 4\ (mod\ 5) \\ p\equiv 1,\ 2,\ 4\ (mod\ 7) \end{cases}$$

$$(2)\ \begin{cases} p \equiv 1 \pmod 3 \\ p \equiv 2,\ 3 \pmod 5 \\ p \equiv 3,\ 5,\ 6 \pmod 7 \end{cases}$$

$$(3)\ \begin{cases} p \equiv 2 \pmod 3 \\ p \equiv 1,\ 4 \pmod 5 \\ p \equiv 3,\ 5,\ 6 \pmod 7 \end{cases}$$

$$(4)\ \begin{cases} p \equiv 2 \pmod 3 \\ p \equiv 2,\ 3 \pmod 5 \\ p \equiv 1,\ 2,\ 4 \pmod 7). \end{cases}$$

e Combinationen sind z. B. für die erste Klasse:

$p \equiv 1$ (mod 3,	$\equiv 1$ (mod 5),	$\equiv 1$ (mod 7)
1	1	2
1	1	4
1	4	1
1	4	2
1	4	4

man bekommt nun vermittelst der in §. 8 unter 1) auseinanderge-
ten Methode nach einigen leichten Rechnungen als mit den vorstehen-
6 von einander verschiedenen Combinationen identisch folgende 6
men der Primzahl p:

$$p = 105n + 1$$
$$p = 105n + 16$$
$$p = 105n + 46$$
$$p = 105n + 64$$
$$p = 105n + 79$$
$$p = 105n + 4.$$

z analog verfährt man bei Bildung der den 3 übrigen Klassen ent-
chenden Formen und man findet schliesslich die den verschiedenen 4
sen entsprechenden Formen wie folgt:

(1) $p = 105n +$	1	16	46	64	79	4
(2) $p = 105n +$	52	82	97	73	103	13
(3) $p = 105n +$	101	26	41	59	89	104
(4) $p = 105n +$	92	2	32	8	23	53.

wissen wir aber, dass diese p ohne Ausnahme noch unter der Form
-1 stehen, d. h. nach dem Modul 4 den Rest +1 lassen. Indem

wir also die früheren Formen mit der letztgenannten combiniren, bekommen wir den Eintheilungsmodul

$$4q = 4 . 105 = 420$$

und, wenn wir nach der absoluten Grösse ordnen, folgende Endresultate:

(1)	$p = 420n + 1$	109	121	169	289	361
(2)	$p = 420n + 13$	73	97	157	313	397
(3)	$p = 420n + 41$	89	101	209	269	341
(4)	$p = 420n + 53$	113	137	197	233	317

II. Die Primzahl p ist von der Form $4n - 1$.

In diesem Falle ist

$$\left(\frac{-3}{p}\right) = (-3)^{\frac{p-1}{2}} = -3^{\frac{p-1}{2}} = -\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right),$$

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right), \quad \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$$

und es wird mithin

$$\left(\frac{-105}{p}\right) = \left(\frac{p}{3}\right) \cdot \left(\frac{p}{5}\right) \cdot -\left(\frac{p}{7}\right).$$

Die 4 Variationen der Vorzeichen rechts, welche die verschiedenen 4 Klassen bestimmen, sind demgemäss:

(1)	$\left(\frac{p}{3}\right) = -1;$	$\left(\frac{p}{5}\right) = -1;$	$\left(\frac{p}{7}\right) = -1$
(2)	-1	$+1$	$+1$
(3)	$+1$	-1	$+1$
(4)	$+1$	$+1$	-1

und die 4 Systeme von Congruenzen, deren Combination die Formen der einzelnen Klassen liefern, werden:

$$(1) \begin{cases} p \equiv 2 \pmod 3 \\ p \equiv 2, 3 \pmod 5 \\ p \equiv 3, 5, 6 \pmod 7 \end{cases}$$

$$(2) \begin{cases} p \equiv 2 \pmod 3 \\ p \equiv 1, 4 \pmod 5 \\ p \equiv 1, 2, 4 \pmod 7 \end{cases}$$

$$(3) \begin{cases} p \equiv 1 \pmod 3 \\ p \equiv 2, 3 \pmod 5 \\ p \equiv 1, 2, 4 \pmod 7 \end{cases}$$

$$(4)\quad \begin{cases} p \equiv 1 \pmod{3} \\ p \equiv 1,\ 4 \pmod{5} \\ p \equiv 3,\ 5,\ 6 \pmod{7}. \end{cases}$$

Hieraus erhalten wir die folgenden Formen als den einzelnen Klassen entsprechende:

(1)	$p = 105n+17$	47	62	38	68	83
(2)	$p = 105n+71$	86	11	29	44	74
(3)	$p = 105n+22$	37	67	43	58	88
(4)	$p = 105n+31$	61	76	94	19	34

oder, wenn wir dieselben auf die Form $4n-1$ transformiren und wieder nach der absoluten Grösse ordnen:

(1)	$420n+47$	83	143	167	227	383
(2)	$420n+11$	71	179	191	239	359
(3)	$420n+43$	67	127	163	247	403
(4)	$420n+19$	31	139	199	271	391.

Hiermit sind alle Formen der Primzahl p gefunden, welche die Fähigkeit haben Divisoren des Ausdruckes x^2+105 werden zu können. Alle übrig bleibenden Formen von Primzahlen können überhaupt nicht Divisoren dieses Ausdruckes werden. Es lässt sich also z. B. die Gleichung

$$11z-105 = x^2$$

unter allen Umständen auflösen, weil 11 unter den Divisoren von x^2-105 ist; dagegen die Gleichung

$$17z-105 = x^2$$

ist unmöglich, weil sich 17 nicht unter den Divisoren von x^2+105 vorfindet, und wir wissen daher im Voraus, dass alles Probiren zu Nichts führen würde. In Betreff der ersten Gleichung findet man leicht, dass die beiden Werthe

$$z = 11,\ x = 4$$

Lösungen derselben sind und ebenso auch die beiden Werthe

$$z = 14,\ x = 7.$$

Wir bemerken noch, dass die sämmtlichen Divisoren des Ausdruckes x^2-q mit Nothwendigkeit auch Divisoren des Ausdruckes

$$x^2-qy^2$$

sein müssen; denn wir wissen nach dem was vorhergeht, dass, wenn q ein Rest von p ist, daraus mit Nothwendigkeit auch qy^2 als Rest von p sich ergiebt.

Beispiel 2. Die Divisoren des Ausdruckes x^2-30 sind nach der absoluten Grösse geordnet folgende 16:

$p=120n+$ 1 7 13 17 19 29 37 49
71 83 91 101 103 107 113 119.

Beispiel 3. Die Divisoren des Ausdruckes x^2+58 sind folgende:

$p=232n+$ 1 9 15 21 25 31 33 35
37 39 47 49 51 55 57 59
61 65 67 69 77 79 81 83
85 91 95 101 107 115 119 121
123 127 129 133 139 135 143 157
159 161 169 179 187 189 191 205
209 213 215 219 221 225 227 229.

Beispiel 4. Die Divisoren des Ausdruckes x^2+22 sind:

$p=88n+$ 1 9 13 15 19 21 23 25 29 31
35 43 47 49 51 61 71 81 83 85.

Beispiel 5. Die Divisoren des Ausdruckes x^2+57 zerfallen in folgende 4 Klassen:

(1) $p=228n+1$ 25 49 61 73 85 121 157 169
(2) $p=228n+29$ 41 53 65 89 113 173 185 221
(3) $p=228n+31$ 67 79 91 103 127 151 211 223
(4) $p=228n+11$ 23 35 47 83 119 131 191 215.

Vierter Abschnitt.

Von der Auflösung der allgemeinen Congruenz zweiten Grades mit einer Unbekannten.

§. 19.

Aufstellung der theoretischen Grundlage.

1) In dem vorhergehenden Abschnitte haben wir uns mit der Theorie der Congruenz

$$x^2 \equiv R \ (mod\ P)$$

beschäftigt; aber die wesentlichen Feststellungen, zu denen wir gelangt sind, betreffen nur die Unterscheidung der Fälle, in denen die genannte Congruenz möglich oder unmöglich ist, und was die eigentliche numerische Auflösung anbetrifft, so sind wir auf Probiren oder indirecte Methoden angewiesen, welche allerdings in den meisten Fällen rasch und sicher zum Ziele führen, aber eines allgemeinen wissenschaftlichen Charakters entbehren. Man vergleiche hierüber den 6ten Abschnitt der Disquisitiones arithmethicae. Gehen wir näher auf die Natur des angedeuteten Problemes ein, so existiren eine grosse Anzahl von Fällen, in welchen die Lösung vermittelst strenger Methode a priori folgt; aber es bleibt immer wenigstens ein Hauptfall übrig, in welchem wir von der Methode im Stiche gelassen werden und die Auflösung nur durch eine Reihe von Versuchen gefunden werden kann.

Nehmen wir unsere Congruenz als möglich und den Modul als eine Primzahl an, so muss letzterer nothwendig von einer der Formen $4n+1$

oder $4n+3$ sein. Ist er von der Form $4n+3$, so hat man die Bedingungscongruenz

$$R^{2n+1} \equiv 1, \text{ also } R^{2n+2} \equiv R \ (mod\ P)$$

und mithin sind die beiden gesuchten Lösungen

$$x \equiv \pm R^{n+1} \ (mod\ P).$$

Ist dagegen P von der Form $4n+1$, so sind die beiden Specialformen $8n+5$ und $8n+1$ zu unterscheiden.

Im ersten Falle gilt die Congruenz

$$R^{4n+2} \equiv 1, \text{ oder } (R^{2n+1}+1)(R^{2n+1}-1) \equiv 0 \ (mod\ P)$$

und es ist daher, je nachdem der erste oder der zweite Factor der Congruenz 0 genügt,

$$x \equiv \mp R^{n+1} \ (mod\ P).$$

Im zweiten Falle, wenn P die Form $8n+1$ hat, sei 2^{μ} die höchste in n enthaltene Potenz von 2 und mithin n von der Form $2^{\mu}(2m+1)$: dann ist die Bedingungscongruenz

$$R^{4 \cdot 2^{\mu}(2m+1)} \equiv 1 \ (mod\ P).$$

Sollte sich nun durch Probiren herausstellen, dass die Congruenz

$$R^{2m+1} \equiv 1, \text{ also } R^{2m+2} \equiv R \ (mod\ P)$$

besteht, so hat man

$$x \equiv \pm R^{m+1} \ (mod\ P);$$

wenn dagegen diese Congruenz nicht besteht, so existirt überhaupt keine ungerade Potenz von R, welche 1 geben und demgemäss zu einer Lösung für x führen könnte*). Mithin müssen wir den gesuchten kleinsten Werth von x, dessen Quadrat die Zahl R um ein Vielfaches von P übertrifft, durch directe Versuche bestimmen, d. h. wir müssen nach einander die Glieder der Reihe

$$P+R \quad 2P+R \quad 3P+R \ \ldots\ldots \ kP+R \ \ldots\ldots$$

---

*) Gäbe es ungerade Potenzen von R, welche 1 zum Reste liessen und wäre die kleinste darunter R^{2h+1}, so wäre $2h+1$ der zu der Zahl R gehörige Exponent. Denn gäbe es einen kleineren Exponenten, welcher die Congruenz 1 befriedigt, so könnte derselbe nur gerade und müsste ein Theiler von $2h+1$ sein, was nicht angeht. Wenn aber R zu $2h+1$ gehört, so muss $2h+1$ ein Theiler von $P-1 = 8 \cdot 2^{\mu}(2m+1)$ sein und dies ist nicht anders möglich, als indem $2h+1$ die Zahl $2m+1$ theilt. Dies aber würde, gegen die Voraussetzung, die Congruenz $R^{2m+1} \equiv 1 \ (mod\ P)$ zur Folge haben.

untersuchen, bis wir auf ein vollkommenes Quadrat stossen. Da der kleinste Werth von x absolut genommen unter $\frac{1}{2}P$ ist, so wird diese Untersuchung nur auf solche Glieder der Reihe auszudehnen sein, die kleiner als $\frac{1}{4}P^2$ sind und die Zahl der Versuche nicht über $\frac{1}{2}P$ steigen. Aber immerhin bleibt die Rechnung äusserst weitläufig und die Beschränkung der Versuche äusserst wünschenswerth. Dies ist in der neuesten Zeit von Desmarest geleistet und wenn er selber den theoretischen Werth seiner Methode vielleicht zu hoch anschlägt, so ist sie doch ohne Zweifel praktisch und auch sonst geeignet die Einsicht des Anfängers in das Wesen der Zahlentheorie zu fördern. Sie ist niedergelegt in einem auch weiter unten von uns benutzten Werke, dessen Titel „Théorie des nombres par E. Desmarest. Paris 1852" ist, und indem wir uns anschicken eine kurze Analyse von der Arbeit des erwähnten Gelehrten zu geben, bemerken wir, dass wir, bei Feststellung der theoretischen Grundlage, im Interesse der Kürze und Uebersichtlichkeit einen selbstständigen Gang einschlagen zu müssen gemeint haben.

2) Die allgemeinste Form der Congruenz zweiten Grades, nämlich

$$AX^2+BX+C \equiv 0 \ (mod\ P)$$

geht durch Multiplication mit einem vermöge der Congruenz

$$2mA \equiv 1 \ (mod\ P)$$

bestimmten Factor $2m$ und durch Abstreifung der Vielfachen von P in den dadurch entstehenden neuen Coefficienten von X^2 über in eine Congruenz von der Form

$$X^2+2aX+b \equiv 0 \ (mod\ P),$$

die man auch noch schreiben kann, wie folgt:

$$(X+a)^2+b-a^2 \equiv 0 \ (mod\ P).$$

Wir kommen mithin, indem wir

$$x = X+a, \ R = b-a^2$$

setzen, wieder zurück auf unsere alte Form

$$x^2+R \equiv 0 \ (mod\ P),$$

welche identisch mit der Gleichung

$$(1) \quad x^2+R = Py,$$

in der wir die Grössen R und P als positiv und zwar die erstere als kleiner als P annehmen; denn wäre R negativ oder grösser als P, so könnte man immer ohne die Natur der vorhergehenden Congruenz zu

ändern ein solches Vielfache von P links entweder zu R addiren oder auch davon subtrahiren, dass das neue resultirende R' die gewünschten Eigenschaften besitzt.

Dieses vorausgesetzt haben wir die Gleichung (1) zunächst in Bezug auf die ganzen Zahlenwerthe, welche die Veränderlichen x und y annehmen können, zu discutiren. Da aber y und P genau in der nämlichen Weise in die Gleichung hineingehen, so liegt der Gedanke nahe, auch P variiren zu lassen und hiernach bleibt blos die Grösse R als eine unveränderliche Zahl übrig, die 3 Grössen x, y, P dagegen können unendlich viele Zahlenwerthe annehmen und es entsteht die Frage, unter welche Formen dieselben sich stellen.

Verstehen wir unter X, Y, P irgend welche specielle, aber sonst willkürliche Zahlenwerthe, die der Gleichung (1) Genüge thun, so ist zunächst klar, dass aus dieser einen speciellen Lösung in x und y zwei von einander verschiedene (und, wenn P eine Primzahl ist, die einzigen) Systeme von Lösungen folgen; wir erhalten dieselben, indem wir alle Zahlen für x einsetzen, welche nach dem Modul P den Zahlen X und $P-X$ congruent sind und mithin unter der allgemeinen Form $x = NP \mp X$ stehen, wo N irgend eine ganze Zahl bezeichnet. Betreffs des zugehörigen y hat man alsdann $Py = (NP \mp X)^2 + R = N^2P^2 \mp 2NPX + X^2 + R$ oder, wenn wir für X^2+R seinen Werth PY einsetzen und darauf mit P durchdividiren $y = N^2P \mp 2NX + Y$. Demgemäss folgen die beiden Systeme einander entsprechender Zahlenwerthe von x und y:

$$(2) \quad x = NP \mp X, \; y = N^2P \mp 2NX + Y.$$

Um nun auch das P in den Kreis der Veränderung hineinzuziehen, wollen wir die Annahmen treffen:

$$X = n, \; Y = 1, \; P = n^2 + r,$$

wo n irgend eine positive ganze Zahl bezeichnet. Alsdann ergiebt sich durch Substitution dieser Werthe in den Gleichungen (2)

$$(3) \quad \begin{cases} P = n^2 + r \\ x = (n^2+r)N \mp n = (nN \mp 1)n + rN \\ y = (n^2+r)N^2 \mp 2nN + 1 = (nN \mp 1)^2 + rN^2. \end{cases}$$

Nun hören diese Werthe aber nicht auf der Gleichung (1) Genüge zu thun, wenn man die Werthe von y und P mit einander vertauscht. Darnach hat man folgendes System zusammengehöriger Werthe:

$$P = (n^2+r)N^2 \mp 2nN+1 = (nN \mp 1)^2+rN^2$$
$$X = (n^2+r)N \mp n = (nN \mp 1)n+rN$$
$$Y = n^2+r$$

und erhält, indem man in den Gleichungen (2) die Grösse N durch die Grösse N' ersetzt und darauf die Werthe für P, X, Y substituirt, folgende beiden Systeme zusammengehöriger und der Gleichung (1) genügender Werthe:

$$(4) \begin{cases} P = (nN-1)^2+rN^2 \\ x = \left\{(nN-1)^2+rN^2\right\}N' \mp \left\{(nN-1)n+rN\right\} \\ y = \left\{(NN' \mp 1)n-N'\right\}^2+r(NN' \mp 1)^2 \end{cases}$$

$$(4') \begin{cases} P = (nN+1)^2+rN^2 \\ x = \left\{(nN+1)^2+rN^2\right\}N' \mp \left\{(nN+1)n+rN\right\} \\ y = \left\{NN' \mp 1)n+N'\right\}^2+r(NN' \mp 1)^2. \end{cases}$$

Lassen wir jetzt in den Gleichungen (3), (4), (4') die P und y ihre Rollen vertauschen und führen an ihrer Stelle zugleich die gleichnamigen griechischen Buchstaben ein, so erhalten wir folgende 3 Gleichungsreihen:

$$(A) \begin{cases} \eta = n^2+r \\ x = (nN \mp 1)+rN \\ \Pi = (nN \mp 1)^2+rN^2 \end{cases}$$

$$(A') \begin{cases} \eta = (nN-1)^2+rN^2 \\ x = \left\{(nN-1)^2+rN^2\right\}N' \mp \left\{(nN-1)n+rN\right\} \\ \Pi = \left\{NN' \mp 1)n-N'\right\}^2+r(NN' \mp 1)^2 \end{cases}$$

$$(A'') \begin{cases} \eta = (nN+1)^2+rN^2 \\ x = \left\{(nN+1)^2+rN^2\right\}N' \mp \left\{(nN+1)n+rN\right\} \\ \Pi = \left\{(NN' \mp 1)n+N'\right\}^2+r(NN' \mp 1)^2 \end{cases}$$

und dieselben geben, indem wir n unbestimmt lassen, dagegen für N und N' die speciellen Zahlenwerthe

1 2 3 4 5 .....

einsetzen, eine Tabelle, in denen wir aber nur die verschiedenen Werthe von η und Π verzeichnen, weil die Werthe von x aus den genannten

Grössen vermöge einer algebraischen Transformation des Productes $\Pi\eta$ in einen Ausdruck von der Form x^2+R mit Leichtigkeit sich ergeben. Die Zahlenwerthe von η sollen die oberste Horizontalreihe bilden und Hauptzahlen heissen. Die erste Hauptzahl ist demgemäss n^2+r und die dazu gehörigen Werthe von Π, die aus der betreffenden Formel in (A) sich berechnen lassen, indem man die Grösse N der Reihe nach die Werthe 1, 2, 3, 4, ... durchlaufen lässt, bilden die dieser Hauptzahl entsprechende Verticalcolumne. Die folgenden Hauptzahlen werden paarweise aus den Formeln für η in (A') und (A'') erhalten, indem man daselbst gleichfalls der Reihe nach die oben genannten Specialwerthe von N einsetzt. Sie bilden demgemäss eine ins Unendliche fortgehende Reihe. Die entsprechenden Verticalcolumnen fliessen aus den Formeln (A') und (A''), indem man daselbst in den Ausdrücken für P der Grösse N den durch die zugehörige Hauptzahl festgelegten Werth von N ertheilt und darauf N' variiren lässt. Jede Verticalcolumne besteht aus zwei Abtheilungen, von denen die eine auf der linken Seite dem oberen Vorzeichen in den Gleichungen (A), (A'), (A''), die andere auf der rechten Seite dem unteren Vorzeichen in den nämlichen Gleichungen entspricht. Zugleich sind die einzelnen darin enthaltenen Zahlen in einer abgekürzten Art dargestellt. Nämlich in allen Fällen hat man Π von der Form

$$\Pi = \left\{f(n)\right\}^2 + R\,.\,Q^2,$$

wo $f(n)$ irgend eine lineäre Function von n und Q irgend eine positive ganze Zahl bezeichnet. Hiernach hat man nur nöthig die respectiven Formen der Function $f(n)$ in die Verticalcolumne einzutragen, wenn man nur die zugehörigen $R.Q^2$ in eine besondere Verticalcolumne einreiht und dafür Sorge trägt, dass zwei zusammengehörige $R.Q^2$ und $f(n)$ immer in derselben Horizontalreihe stehen.

Bei dieser Einrichtung ist es äusserst leicht, den Werth von N zu bestimmen, der irgend einem Glied der auf die Hauptzahl n^2+R bezüglichen Verticalcolumne entspricht. Man hat nämlich nur zu zählen, welchen Platz das betrachtete Glied in der bezüglichen Verticalreihe, mag sie nun die rechte oder die linke Seite der Columne ausmachen, einnimmt. Ganz in derselben Weise giebt der einer speciellen Function $f(n)$ ent-

sprechende Werth von N' an, das wie vielste Glied in seiner Verticalreihe das betrachtete $f(n)$ ist.

Endlich bemerken wir noch, dass, wenn man in den Formeln (A') und (A'') der Grösse N den speciellen Werth 1 ertheilt, ferner an die Stelle von n respective $n+1$ und $n-1$ treten lässt und hierauf auch noch N' durch $N \pm 1$ ersetzt, beide Systeme von Formeln in die Formeln (A) übergehen. Demnach haben wir bei der Bildung unserer Tabelle nicht nöthig in (A') und (A'') die Substitution $N=1$ vorzunehmen und die in Rede stehende Tabelle nimmt daher folgende Gestalt an:

	(A) N	(A') $N=2$, N'	(A'') $N=2$, N'	(A') $N=3$, N'	(A'') $N=3$, N'
$R.Q^2$	n^2+R	$(2n-1)^2+4R$	$(2n+1)^2+4R$	$(3n-1)^2+9R$	$(3n+1)^2+9R$
$R.\ 1^2$	$n-1$ $n+1$	$n-1$	$n+1$		
$R.\ 2^2$	$2n-1$ $2n+1$			$2n-1$	$2n+1$
$R.\ 3^2$	$3n-1$ $3n+1$	$3n-2$ $3n-1$	$3n+2$ $3n+1$		
$R.\ 4^2$	$4n-1$ $4n+1$			$4n-1$	$4n+1$
$R.\ 5^2$	$5n-1$ $5n+1$	$5n-3$ $5n-2$	$5n+3$ $5n+2$	$5n-2$	$5n+2$
$R.\ 6^2$	$6n-1$ $6n+1$				
$R.\ 7^2$	$7n-1$ $7n+1$	$7n-4$ $7n-3$	$7n+4$ $7n+3$	$7n-2$	$7n+2$
$R.\ 8^2$	$8n-1$ $8n+1$			$8n-3$	$8n+3$
$R.\ 9^2$	$9n-1$ $9n+1$	$9n-5$ $9n-4$	$9n+5$ $9n+4$		
$R.10^2$	$10n-1$ $10n+1$			$10n-3$	$10n+3$
$R.11^2$	$11n-1$ $11n+1$	$11n-6$ $11n-5$	$11n+6$ $11n+5$	$11n-4$	$11n+4$
$R.12^2$	$12n-1$ $12n+1$				

	(A') $N=4$, N'	(A'') $N=4$, N'	(A') $N=5$, N'	(A'') $N=5$, N'	(A') $N=6$, N'
$R.Q^2$	$(4n-1)^2+16R$	$(4n+1)^2+16R$	$(5n-1)^2+25R$	$(5n+1)^2+25R$	$(6n-1)^2+36R$
$R.\ 1^2$					
$R.\ 2^2$					
$R.\ 3^2$	$3n-1$	$3n+1$			
$R.\ 4^2$			$4n-1$	$4n+1$	
$R.\ 5^2$	$5n-1$	$5n+1$			$5n-1$
$R.\ 6^2$			$6n-1$	$6n+1$	
$R.\ 7^2$	$7n-2$	$7n+3$			
$R.\ 8^2$					
$R.\ 9^2$	$9n-2$	$9n+2$	$9n-2$	$9n+2$	
$R.10^2$					
$R.11^2$	$11n-3$	$11n+3$	$11n-2$	$11n+2$	$11n-2$
$R.12^2$					

3) Wir wollen jetzt beweisen, dass, wenn die Gleichung (1), in der wir jetzt unter P irgend eine specielle Zahl verstehen, möglich ist,

immer eine unendliche Menge von Zahlenwerthen Π in unserer Tabelle existiren, welche Vielfache von P sind. In der That, die allgemeine Form irgend eines Π (den Fall der ersten Verticalcolumne mit eingerechnet) ist $\{(NN'\mp1)n\mp N'\}^2+R(NN'\mp1)^2$ und damit es ein Vielfaches von P darstelle, ist nothwendig und hinreichend, dass sich für n, N, N' solche ganze und positive Zahlenwerthe bestimmen lassen, vermöge deren die Congruenz

$$(5)\quad \{(NN'\mp1)n\mp N'\}^2 \equiv -R(NN'\mp1)^2 \pmod P$$

befriedigt wird. Bestimmen wir uns hier zunächst die Grössen N und N' derartig, dass $NN'\mp1$ eine relative Primzahl zu P wird. Indem man eine solche mit m bezeichnet, ist dazu hinreichend, dass man $NN'\mp1=m$ setze, also $N'=\frac{m\pm1}{N}$ und nun für N alle nur möglichen Theiler von $m\pm1$ einsetzt. Namentlich ist hier die specielle Annahme $N=1$ als unter allen Umständen zum Ziele führend zu bemerken, weil daraus, mit Rücksicht auf das Nachfolgende, sich ergiebt, dass in der ersten Verticalcolumne eine unendliche Menge von Gliedern existiren, welche Vielfache von P sind.

Dieses vorausgesetzt ist $(NN'\mp1)^2$ unter allen Umständen ein Rest von P. Denn seien die Primfactoren von P dargestellt durch die Symbole a, b, c, ..., so dass man $P=a^\alpha, b^\beta, c^\gamma$, ... hat, so ist nach dem Satze unter c) p. 227 der genannte Ausdruck ein Rest der einzelnen Factoren a, b, c, ...; mithin weiter auch (cf. p. 214) ein quadratischer Rest der Potenzen a^α, b^β, c^γ, ..., und endlich (nach einem p. 207 befindlichen Satze) auch von dem Producte P. Ferner ist $-R$ ein quadratischer Rest von P, weil wir die Congruenz $x^2+R\equiv0 \pmod P$ als möglich voraussetzen. Dies beides zusammengenommen ergiebt, dass der Ausdruck $-R(NN'\mp1)^2$, welcher die rechte Seite der Congruenz (5) ausmacht, gleichfalls ein quadratischer Rest von P ist. Dies heisst nichts anderes als der Ausdruck auf der linken Seite in (5), nämlich $(NN'\mp1)n\mp N'$ kann eine unendliche Menge von Zahlenwerthen annehmen, welche Lösungen der Congruenz (5) sind. Sei die kleinste darunter x', so darf man, indem M eine beliebige positive oder negative Zahl bezeichnet, die Gleichung

$$(6)\quad (NN'\mp1)n\mp N'=x'+MP$$

setzen. Da hier nun die N, N', n, P, x' lauter bestimmte, wenn auch zum Theil willkürliche (namentlich ist die Menge zusammengehöriger Werthe von N und N' unbegrenzt) Zahlen sind, so bleiben in dieser Gleichung nur zwei Zahlen n und M übrig, welche unbestimmt sind. Da sie indessen nur in der ersten Potenz darin vorkommen, so lässt sich eine unendliche Menge einander entsprechender Zahlenwerthe von n und M finden, welche ihr Genüge leisten. Namentlich wird, da M sowohl positiv wie negativ sein kann, eine gleichfalls unbegrenzte Menge positiver Zahlenwerthe der Grösse n existiren. Also jeder der unendlich vielen statthaften Annahmen über die N und N' entsprechen gleichfalls unendlich viele Zahlenwerthe von n, d. h. das durch ein specielles N' festgelegte Glied der Nten Verticalcolumne stellt für einen durch die Congruenz

$$(7) \quad (NN' \mp 1)n \mp N' \equiv x' \pmod{P}$$

festgelegten Werth von n ein Vielfaches von P dar.

Hiermit ist das Theorem bewiesen, dass, wenn die Gleichung $x^2 + R = Py$ möglich ist, in den Verticalreihen unserer Tabelle eine unendliche Menge von Zahlen Π sich verzeichnet finden, welche Vielfache von P darstellen, so dass man Π von der Form mP hat. Insbesondere sind solche Zahlen allemal in der ersten Verticalreihe anzutreffen.

Nehmen wir nun an, wir hätten ein solches Vielfaches von P in der Tafel gefunden, so führt die Kenntniss der Stelle, an der es steht, unmittelbar zu einer Lösung der gegebenen Gleichung. Zu dem Zwecke brauchen wir uns nur auf einen Satz zu beziehen, der aus der Anlage der Entwickelung, welche uns zu den Gleichungen (A), (A'), (A''), geführt hat, unmittelbar folgt, dass jede einer Verticalcolumne angehörige Zahl mit ihrer Hauptzahl multiplicirt ein Product von der Form $x^2 + R$ liefert.

In der That sei Π die betrachtete specielle Zahl von der Form mP: so ist sie doch in der Tafel unter der Form

$$\left\{ f(n) \right\} + R^2 : Q^2$$

in der bekannten Weise dargestellt und die Untersuchung der Stelle, an der sich $f(n)$ befindet, führt unmittelbar zur Bestimmung der Zahlenwerthe

von N und N', welche sich auf das betrachtete Vielfache von P beziehen; die Zahl n endlich wird gefunden, indem wir die Gleichung

$$f(n) = \sqrt{mP - R.Q^2}$$

nach n auflösen. Nun ist weiter $H\eta = mP\eta$ ein Product von der Form x^2+R und die speciellen Zahlenwerthe von η und x werden berechnet, indem man in den allgemeinen Ausdrücken unter (A), (A') oder (A'') für N, N', n die gefundenen speciellen Zahlenwerthe einsetzt. Dies vorausgesetzt besteht die Gleichung

$$x'^2+R = mP\eta',$$

indem x' und η' die durch die angedeuteten Substitutionen erhaltenen Zahlenwerthe von x und η bezeichnen; d. h. wir haben die particuläre Lösung der vorgegebenen Gleichung

$$x = x', \; y = m\eta'.$$

4) Aus den vorstehenden Entwickelungen fliesst nun folgende Auflösungsmethode. Wenn die gegebene Gleichung möglich ist, so existiren im Allgemeinen immer solche Zahlen mP (wo m auch der Einheit gleich sein kann), die unter der Form $U^2+R.Q^2$ stehen; daraus folgt weiter

$$mP - R.Q^2 = U^2.$$

Um nun für irgend ein specielles m, am einfachsten $m=1$, die Zahl Q zu bestimmen, welche die Differenz auf der linken Seite zu einem vollständigen Quadrate macht, untersuche man der Reihe nach die Differenzen

$$mP - R.1^2, \; mP - R.2^2, \; mP - R.3^2, \; \ldots\ldots,$$

bis man auf eine solche stösst, welche die gewünschte Eigenschaft hat. Sei diese Differenz $mP - R.Q^2$, wo Q eine durch die bezeichneten Versuche bestimmte Zahl bezeichnet, so wird man in der durch den Rest $R.Q^2$ bestimmten Horizontalreihe sich diejenige Function von n aussuchen, welche die Gleichung $f(n) = U$ dergestalt befriedigt, dass n sich als eine ganze positive Zahl bestimmt, und da man die Werthe von N und N' aus der Stelle sich entnehmen kann, welche $f(n)$ in der Tafel einnimmt, so hat man alle Elemente nur vermöge der Formeln (A), (A') oder (A'') die Werthe von x und η und mithin die particuläre Lösung $x = x$ und $y = m\eta$ sich zu berechnen. Man sieht leicht ein, dass die angedeutete Versuchsreihe eine sehr begrenzte ist; einmal ist sie begrenzt durch die Natur der Zahl P selbst; denn offenbar wird die äusserste

Grenze, bis zu der hin man kommen kann, diejenige ganze Zahl Q sein, für welche die Differenz $mP-R.Q^2$ anfängt negativ zu werden. Weiter aber werden die Versuche auch sehr abgekürzt (durch Beseitigung der Quadratwurzelausziehungen, welche mit den einzelnen Gliedern unserer Differenzenreihe vorgenommen werden müssen), wenn man bemerkt, dass alle solche Glieder der Differenzenreihe, die auf eine der Ziffern

$$2,\ 3,\ 7,\ 8$$

ausgehen, unbedingt keine vollständigen Quadrate geben können. Indessen werden wir weiter unten Näheres über die Mittel beibringen, die zur Lösung erforderliche Versuchsreihe abzukürzen und wollen zuvor nur noch, um das Verständniss zu erleichtern, ein Beispiel durchrechnen.

Sei die vorgelegte Gleichung

$$x^2+254 = 4689y,$$

so ist die zu betrachtende Differenzreihe

$$P-R = 4435,\ P-4R = 3673,\ P-9R = 2403,\ P-16R = 625.$$

Das erste Glied derselben ergiebt sich durch den Versuch der Wurzelausziehung oder auch zu Folge der Bemerkung, dass eine auf 5 ausgehende Zahl nur dann ein vollständiges Quadrat sein kann, wenn die vorletzte Ziffer eine 2 ist, als irrational; ebenso ist das zweite und dritte Glied wegen der Natur der letzten Ziffer irrational; das vierte Glied dagegen hat zur Quadratwurzel die Zahl 25. Hiernach ist

$$4689-254.4^2 = 25^2,\ Q=4,\ U=25.$$

Sucht man jetzt in der durch die Aufschrift $R.4^2$ bestimmten Horizontalreihe nach solchen Formen der linearen Function $f(n)$, welche, indem n eine ganze Zahl darstellt, der Zahl U gleich werden können, so genügt dieser Eigenschaft die Form $4n+1$. Betrachtet man diese Form als der ersten Verticalcolumne angehörig, so findet man

$$n=6,\ N=4.$$

Die Formeln (A) liefern dann weiter für das untere Vorzeichen

$$y=m\eta=\eta=6^2+254=290,\quad x=25.6+254.4=1166.$$

Betrachtet man $4n+1$ als eine Zahl der fünften Verticalcolumne, so hat man $n=6$, $N'=1$, $N=3$ und die Formeln (A'') liefern für das untere Vorzeichen

$$x = (19^2+254.9).1+(19.6+254.3) = 3523,$$

$$y = \eta = 19^2+254.9 = 2647.$$

Die Anwendung endlich der Form $4n+1$ als einer Form der neunten Verticalcolumne ergiebt $n=6$, $N'=1$, $N=3$ und die Formeln (A'') liefern für das obere Vorzeichen die folgende particuläre Lösung:

$$x = (31^2+254.25)-(31.6+254.5) = 2855$$

$$y = \eta = 31^2+254.25 = 7311.$$

Die zuerst gefundene particuläre Lösung für x führt auf folgende beiden allgemeinen, die von einander verschieden sind:

$$x \equiv 1166,\ 3523 \ (mod\ 4689)$$

und ganz die nämlichen Lösungen fliessen auch aus den beiden anderen particulären.

Da der Modul P eine Zerlegung in die Primfactoren $3.3.521 = 3^2.521$, also im Ganzen zwei ungleiche Primfactoren enthält, so müssen nach einer am Schlusse der zweiten Abtheilung p. 205 gemachten Bemerkung 4 von einander verschiedene Lösungen der gegebenen Gleichung existiren. Es fragt sich, wie man die beiden noch übrigen Lösungen findet. Es bedarf dazu keiner Versuche, sondern sie können vermittelst strenger Methode bestimmt werden. Unsere Gleichung ist doch identisch mit der Congruenz

$$x^2 \equiv -254 \ (mod\ 9.521)$$

und zerfällt in die beiden Congruenzen:

$$x^2 \equiv -254 \ (mod\ 9) \text{ und } x^2 \equiv -254 \ (mod\ 521).$$

Von jeder dieser beiden Congruenzen ist eine Lösung $x \equiv 1166$, mithin ist die andere $x \equiv -1166$. Drückt man diese Lösungen in den kleinsten Zahlen aus und setzt die Lösungen der ersten Congruenz gleich ϱ', die der zweiten gleich ϱ'', so hat man

$$\varrho' \equiv +4,\ -4 \ (mod\ 9)$$

$$\varrho'' \equiv +124,\ -124 \ (mod\ 521).$$

Löst man sich nun in Befolgung der Regeln p. 196 und 197 die beiden Hülfscongruenzen $m'.521 \equiv 1$ (mod 9 und $m''.9 \equiv 1$ (mod 521) auf, so findet man $m' = -1$, $m'' = +58$ und weiter

$$x \equiv -521\varrho' + 521\varrho'' \ (mod\ 4689).$$

Indem man hier an Stelle von ϱ' und ϱ'' ihre Werthe einsetzt und die verschiedenen möglichen Combinationen bildet, folgen die 4 Lösungen:

$$x \equiv \begin{cases} -521.4+522.124 = & 62644 \equiv & 1687 \\ -522.124 = & -66812 \equiv & -1166 \\ +521.4+522.124 = & 66812 \equiv & 1166 \\ -522.124 = & -62644 \equiv & -1687 \end{cases} (mod\ 4689).$$

Der ersten unter diesen 4 Lösungen entspricht das System der Werthe $x = 1687$ und $y = 607$.

Man sieht leicht ein, dass die an dem vorstehenden Beispiele erörterte Methode allgemeiner Natur und dass um alle möglichen von einander verschiedenen Lösungen einer Congruenz zweiten Grades zu erlangen, man nur nöthig hat irgend eine specielle zu finden. Mithin ist allein die praktische Schwierigkeit zu beseitigen, welche sich der Aufsuchung einer Lösung entgegenstellt und welche wesentlich in der Menge der hierzu erforderlichen Versuche besteht. Die Zahl dieser Versuche möglichst zu vermindern ist der Zweck der weiter unten folgenden Auseinandersetzungen.

§. 20.

Beschränkung der zur Auflösung der Gleichung $x^2+R=Py$ erforderlichen Versuche.

Wenn die Gleichung $x^2+R=Py$, wo R und P positiv und $R<P$ möglich ist, so existirt im Allgemeinen immer eine Zahl U, welche positiv und kleiner als P ist, von der Beschaffenheit, dass die Gleichheit

$$(1) \quad Pm = U^2+R.Q^2 \text{ oder } Pm-RQ^2 = U^2$$

erfüllt wird, indem m nicht über $\frac{P}{16}+3$ und Q nicht über 3 hinausgeht.

Um den Beweis dieses Theoremes einigermassen abzukürzen wollen wir den Modul P als eine ungerade Zahl betrachten und haben dann die beiden Fälle zu unterscheiden: $P=4q+1$ und $P=4q-1$, von denen wir namentlich den ersten mit aller Ausführlichkeit durchnehmen werden.

1) Es sei P von der Form $4q+1$.

Zunächst bemerken wir, dass, wenn wir unter x und y diejenigen speciellen Zahlen verstehen, welche particuläre Lösungen unserer Gleichung in den kleinsten Zahlen darstellen, die Grösse x nicht den Werth

$2q$ und die Zahl y nicht den Werth q übersteigen darf. Das erste bedarf wohl keines Beweises; das zweite erhellt daraus, dass, wenn in der Gleichung

$$(2)\quad x^2+R=(4q+1)y$$

$x \leqq 2q$ ist, nothwendig, indem man an Stelle von x^2 den Werth $(2q)^2$ und an Stelle von R den grösseren Werth $4q+1$ treten lässt, die Ungleichheit $4q^2+4q+1>(4q+1)y$ folgt; hieraus $y<q+\frac{3q+1}{4q+1}$, d. h., da der Bruch rechts keine Ganzen enthält, es ist y kleiner als q. Für unseren Zweck ist es daher hinreichend nur solche Werthe von y zu untersuchen, welche positiv und kleiner als q sind.

Denken wir uns für y alle die verschiedenen Zahlenwerthe, die unterhalb dieser Grenzen liegen, eingesetzt und betrachten darunter, indem k eine der Zahlen 0, 1, 2, 3 bezeichnet, zuerst die folgende Partie:

$$1\ \ 2\ \ 3\ \ 4\ \ \ldots\ldots\ \frac{q-k}{4}+3,$$

so wird entweder eine unter diesen Zahlen der Gleichung (2) Genüge leisten, etwa die Zahl m, oder es ist keine, die dieses thut, darunter. Im ersten Falle ist unser Theorem verificirt und zwar für den speciellen Fall $Q=1$. Denn m ist eine Zahl $\overline{\overline{<}}\frac{q-k}{4}+3$ und mithin nach der Voraussetzung über die Natur der Grösse k, auf jeden Fall $<\frac{P}{16}+3$.

Im zweiten Falle dagegen kann man versichert sein, dass die in Frage stehende Lösung nach y nothwendig eine der Zahlen $\frac{q-k}{4}+4$, $\frac{q-k}{4}+5$, ... $q-3$, $q-2$, $q-1$, q ist. Nehmen wir der grösseren Einfachheit halber an, dass, unter Beibehaltung der über die Natur von k gemachten Voraussetzung, auch die absteigende Reihe der Zahlen q, $q-1$, $q-2$, ... $q-k$ keiner Lösung nach y entspreche: dann muss der gesuchte Werth von y nothwendig zwischen den Zahlen $\frac{q-k}{4}+3$ und $q-k$ liegen; mithin, indem wir in (2)

$$y=\frac{q-k}{4}+n$$

setzen, wird die Gleichung

$$(4q+1)\left(\frac{q-k}{4}+n\right)=x^2+R$$

thwendig befriedigt werden müssen durch irgend einen der folgenden hlenwerthe für n: 4, 5, 6, ... $q-k-\frac{q-k}{4}$; d. h. die Zahl n ist ischen den Zahlen 4 und $3 \cdot \frac{q-k}{4}$ enthalten. Diesem speciellen Zahnwerthe von n entspricht nun ein Werth von x, der, indem δ eine sitive und in keinem Falle über n hinausgehende Zahl bezeichnet, von er Form $q+2n-\delta$ ist.

Um dieses zu beweisen gehen wir von den beiden Identitäten

$$(4q+1)\left(\frac{q-k}{4}+n\right)=(q+n)^2 \qquad +\left(2qn+n-n^2-qk+\frac{q-k}{4}\right)$$

nd

$$(4q+1)\left(\frac{q-k}{4}+n\right)=(q+2n+1)^2-\left(\frac{7q}{4}+qk+4n^2+3n+\frac{k}{4}+1\right)$$

s. In der ersten Identität ist das zweite Glied der rechten Seite im lgemeinen stets grösser als R. Es ist nämlich, wegen der für sich identen Ungleichungen $2qn+n-n^2-qk+\frac{q-k}{4}<2q(n+1)+(n+1)-$ $+1)^2-qk+\frac{q-k}{4}$ und $2qn+n-n^2-qk+\frac{q-k}{4}>2qn+n-n^2-$ $k+1)+\frac{q-k-1}{4}$ klar, dass dasselbe mit wachsenden n zunimmt und it wachsenden k abnimmt. Demgemäss ist im ungünstigsten Falle, der ntreten kann, $n=4$ und $k=3$. Unter dieser Annahme reducirt sich er unser Ausdruck auf $8q-12-3q+\frac{q-3}{4}=\frac{21q-51}{4}$ und der Werth eser Quantität bleibt, wenigstens wenn man $q>10$ annimmt, stets unrhalb der Grenze $4q$ und daher auch unterhalb R. Da nun die rechte eite unserer ersten Identität denselben Zahlenwerth haben muss, wie die nke Seite der Gleichung (2), so ist wegen des Verhältnisses der Uneichheit, welches zwischen den zweiten Gliedern dieser beiden Ausrücke eintritt, nothwendig $q+n<x$.

Aus der zweiten Identität folgt, da das zweite Glied rechts stets neativ ausfällt, wenn anders, wie es sein muss, die rechte Seite gleich ^2+R werden soll, $x<q+2n+1$. Es bestehen also die beiden Unleichungen

$$q+n<x<q+2n+1$$

und es muss daher x von der behaupteten Form $q+2n-\delta$ sein, so dass δ höchstens gleich n wird.

Indem also das System der Werthe

$$y=\frac{q-k}{4}+n,\quad x=q+2n-\delta$$

die particuläre Lösung der Gleichung (2) in den kleinsten Zahlen darstellt, können wir dieselbe uns jetzt auch durch eine Gleichung der folgenden Form

$$(3)\qquad (4q+1)\left(\frac{q-k}{4}+n\right)=(q+2n-\delta)^2+R$$

ersetzt denken und zwar sind die Voraussetzungen, unter denen diese Gleichung besteht, folgende: zuerst, dass keine der Zahlen $-\left(\frac{q-k}{4}-1\right)$, $-\left(\frac{q-k}{4}-2\right)$, ... -2, -1, 0, 1, 2, 3, für n eingesetzt ihr Genüge leistet und mithin n zwischen den Grenzen 4 und $3 . \frac{q-k}{4}$ liegt, und dann weiter, dass die ganze und positive Zahl δ die Zahl n in keinem Falle übersteigt.

Dies vorausgesetzt kann man beweisen, dass, wenn man die Gleichung (3) mit einer der beiden Quadratzahlen 4 oder 9 multiplicirt, sie in eine Gleichung entweder von der Form

$$Pm=U^2+R.2^2$$

oder von der Form

$$Pm=U^2+R.3^2$$

transformirt wird, mit der für uns wesentlichen Bedingung, dass der Coefficient m von P in der transformirten Gleichung nicht grösser als $\frac{q-k}{4}+3$ und also auf jeden Fall unterhalb der Grenze $\frac{P}{16}+3$ liegt. Hiermit ist dargethan, dass, wenn die Gleichung

$$Pm=U^2+R.1^2$$

nicht stattfindet, indem m zwischen den Grenzen 0 und $\frac{P}{16}+3$ enthalten ist, nothwendig, indem m zwischen den nämlichen Grenzen bleibt, eine der vorhergehenden Gleichungen besteht, d. h. unser Theorem ist als richtig erwiesen.

Multipliciren wir (3) mit 4, so folgt nach einander $(4q+1)(q-k+4n)$ $=(2q+4n-2\delta)^2+R.2^2$; $(4q+1)(4q+1-3q-1-k+4n)=(4q+1+$

$\overline{4n-2\delta-2q-1})^2+R.2^2$ oder, wenn man nach Potenzen von $4q+1$ ordnet,

$$(4)\quad (4q+1)\left\{q-k-(4n-4\delta-1)\right\}=\left\{4n-(2\delta+2q+1)\right\}^2+R.2^2,$$

und, wenn diese Gleichung eine solche Lösung geben soll, die den Bedingungen unseres Theoremes entspricht, so ist die erforderliche und zureichende Bedingung das Stattfinden der Ungleichung $q-k-(4n-4\delta-1) \overline{\overline{<}} \frac{q-k}{4}+3$, welche identisch ist mit der folgenden

$$(5)\quad 4(n-\delta) \geqq 3\,\frac{q-k}{4}-2.$$

Multipliciren wir (3) dagegen mit 9, so erhalten wir $(4q+1)\left(\frac{9q-9k}{4}+9n\right) = (3q+6n-3\delta)^2+R.3^2$ oder wenn man entwickelt und dabei nach Potenzen von $4q+1$ ordnet:

$$(6)\quad (4q+1)\left\{\frac{q-k}{4}+6\delta-3n-2k+1\right\}=(6n-3\delta-q-1)^2+R.3^2$$

und damit hier die linke Seite ein Vielfaches des Moduls P von der erforderlichen Art darstelle, ist die erforderliche und zureichende Bedingung, dass man habe $\frac{q-k}{4}+6\delta-3n-2k+1 \overline{\overline{<}} \frac{q-k}{4}+3$ oder $\delta \overline{\overline{<}} \frac{n}{2}+\frac{k+1}{3}$, oder, da k nach unserer Annahme den Zahlenwerth 2 nicht übersteigt, also in dem Bruche $\frac{k+1}{3}$ höchstens ein einziges Ganzes enthalten sein kann,

$$(7)\quad \delta \overline{\overline{<}} \frac{n}{2}+1,\ 2n-\delta \geqq \frac{3n}{2}-1.$$

Es lässt sich nun zeigen, dass, wenn n und δ den gedachten Voraussetzungen unterworfen bleiben, die Ungleichungen (5) und (7) mit einander unverträglich sind, so dass, wenn die eine besteht, die andere nicht besteht, und dass mithin nothwendig stets eine von ihnen erfüllt werden muss, d. h. die zugehörige Gleichung hat die von dem Theorem geforderte Form.

Nehmen wir an, die Ungleichheit (7) werde nicht erfüllt, sondern man habe

$$(8)\quad \delta > \frac{n}{2}+1,\ 2n-\delta < \frac{3n}{2}-1;$$

dann ist unmittelbar klar, dass den Werth der Wurzel x in (2) oder,

was das Nämliche ist, der Werth von $q+2n-g$ in (3) unterhalb der Grenze $q+\frac{3n}{2}-1$ liegt; mithin wird man diese Wurzel darstellen können durch einen Ausdruck von der Form $q+\frac{3n}{2}-h$, wo h eine Zahl zwischen den Grenzen 1 und $\frac{n}{2}$ sein muss, so jedoch, dass es keinen dieser Grenzwerthe erreichen darf. Setzen wir diesen Werth in (3) ein, so kommt

$$(9)\quad (4q+1)\left(\frac{q-k}{4}+n\right)=\left(q+\frac{3n}{2}-h\right)^2+R.$$

Indem wir den Werth von h aus dieser Gleichung berechnen, können wir die Grösse R vernachlässigen. Setzen wir nämlich den aus solcher Vernachlässigung entspringenden Werth von h gleich h', so haben wir

$$(4q+1)\left(\frac{q-k}{4}+n\right)=\left(q+\frac{3n}{4}-h'\right)^2.$$

Da nach unserer obigen Auseinandersetzung der Werth der linken Seite zwischen $(q+n)^2$ und $(q+2n+1)^2$ enthalten sein muss, so folgt, dass h' zwischen den Grenzen $-\frac{n}{2}$ und $+\frac{n}{2}+1$ liegt, ohne dieselben jedoch erreichen zu können; mithin ist sein absoluter Werth, wie der von h, jedenfalls nicht über $\frac{n}{2}$ und daher $h+h'$ eine Grösse, welche die Zahl n nicht übersteigt. Nun folgt aus unseren beiden letzten Gleichungen $\left(q+\frac{3n}{2}-h'\right)^2=\left(q+\frac{3n}{2}-h\right)^2+R$ oder, da R kleiner als $4q+1$ ist, $\left(q+\frac{3n}{2}-h'\right)^2<\left(q+\frac{3n}{2}-h\right)^2+4q+1$, mithin nach einigen leichten Entwickelungen

$$h-h'<\frac{4q+1}{2q+3n-(h+h')}.$$

Weil nun $h+h'$ nicht über n ist, so ist der Nenner rechts nicht unter der Grenze $2q+2n$ und mithin jedenfalls grösser als die Quantität $2q+\frac{1}{2}$; demgemäss ist der Werth des ganzen Bruches kleiner als der Werth des Quotienten $\frac{4q+1}{2q+\frac{1}{2}}=2$ und die vorhergehende Ungleichheit zeigt, dass die Differenz $h-h'$ jedenfalls unter 2 bleibt; die Vertauschung der Grössen h und h' ist daher statthaft, da ihre Grenzen sehr nahe zusammenfallen; in der That ist es nicht schwer sich davon zu überzeugen,

dass dadurch die weiter unten zu erwähnende Grenze von q nur um eine Einheit geändert würde.

Entwickeln wir jetzt aus der Gleichung (9) unter Vernachlässigung von R den Werth der Grösse h, so folgt $q+\frac{3n}{2}-h=\sqrt{(4q+1)\left(\frac{q-k}{4}+n\right)}$ (die Quadratwurzel darf nur positiv genommen werden, weil die Grösse $q+\frac{3n}{2}-h$ bei der Beschaffenheit von h nothwendig positiv ist. Also hat man zu Folge der Bedeutung von h $q+2n-\delta=q+\frac{3n}{2}-h$, also $n-\delta=\frac{n}{2}-h$ und

$$4(n-\delta)=2n-4h=-4(q+n)+\sqrt{16q^2+64qn+16n+4(q-k)-16qk}.$$

Wir müssen jetzt zusehen, ob durch den gefundenen Ausdruck für $4(n-\delta)$, indem die Ungleichung (8) besteht, die Ungleichung (5) befriedigt werde oder nicht befriedigt werde, d. h. ob die Ungleichung

$$(10)\qquad -4(q+n)+\sqrt{16q^2+64qn+16n+4(q-k)-16qk}\geqq 3\frac{q-k}{4}-2$$

oder die mit ihr identische

$$\left\{16q^2+64qn+16n+4(q-k)-16qk\right\}-\left\{4(q+n)+3\frac{q-k}{4}-2\right\}^2\geqq 0$$

bestehe oder nicht bestehe. Entwickeln wir uns den Ausdruck linker Hand, so geht er über in

$$(11)\qquad 26qn+(32+6k)n-16n^2-\frac{105q^2}{16}+q\left(23-\frac{71k}{8}\right)-\frac{9k^2}{16}-7k-4$$

und wir haben nun sein Verhalten näher zu untersuchen, wenn man die Grösse n die Reihe der zulässigen Werthe durchlaufen lässt. Nun fallen alle Werthe von n, die zwischen den Grenzen 3 und $3\frac{q-k}{8}-3$ enthalten sind, wie wir weiter unten zeigen werden, als mit der Ungleichung (8), die wir hier als bestehend voraussetzen, unvereinbar aus unserer Untersuchung heraus. Wir haben also nur den Verlauf des Ausdruckes zwischen den Grenzen $n=3\frac{q-k}{8}-3$ und $n=3\frac{q-k}{4}$ zu betrachten. Zu dem Zwecke bemerken wir, dass er innerhalb der genannten Grenzen gleichzeitig mit n wächst. Denn setzt man $n+1$ an Stelle von n und zieht von dem auf diese Weise entstehenden Ausdruck den ursprünglichen ab, so ist der Rest $26q+16+6k-32n$, eine Grösse, die für die in

Anspruch genommenen Werthe von q stets positiv ausfällt. Damit also die Quantität (11) immer positiv bleibe, ist hinreichend, dass sie für die untere Grenze der n, nämlich $3\frac{q-k}{8}-3$, positiv sei. Nun geht sie durch Substitution dieses Werthes für n über in $\frac{15q^2}{16}-q\left(\frac{95k}{8}+7\right)-\left(\frac{27k^2}{4}+73k+244\right)$, oder, wenn man den allerungünstigsten Fall $k=3$ setzt, in $\frac{15q^2+682q-8380}{16}$, ein immer positiver Ausdruck, sobald q die Grenze 55 überschreitet. In weiterer Folge hiervon besteht die Ungleichung (10), welche mit der Ungleichung (5) identisch ist, d. h. gerade dadurch, dass die Ungleichung (7) nicht besteht, wird das Bestehen der Ungleichung (5) bedingt, oder die beiden Ungleichungen (5) und (7) schliessen sich gegenseitig aus, wie wir oben behaupteten.

Es ist aber, um diesen Schluss zu rechtfertigen, noch nachträglich zu untersuchen, inwiefern die obige Voraussetzung Geltung habe, dass für alle solche Werthe von n, die zwischen den Grenzen 3 und $3\frac{q-k}{8}-3$ liegen oder mit andern Worten, die, indem l eine zwischen 3 und $3\frac{q-k}{8}-3$ variirende Zahl bezeichnet, unter der allgemeinen Form $3\frac{q-k}{8}-l$ stehen, die Ungleichung (8) keinen Bestand haben könne.

Aus der Ungleichung (8) folgt $q+2n-\delta<q+\frac{3n}{2}-1$, also, wenn man für n seinen Werth $3\frac{q-k}{8}-l$ einsetzt,

$$q+2n-\delta<\frac{25q}{16}-\left(\frac{9k}{16}+1\right)-\frac{3l}{2}$$

und ebenso leitet man her

$$(4q+1)\left(\frac{q-k}{4}+n\right)=\frac{5q^2}{2}-q.\frac{20k-5}{8}-\frac{5k}{8}-4ql-l.$$

Nun geht aber aus der Gleichung (3) hervor, dass, wenn man das Quadrat der auf der rechten Seite der vorhergehenden Ungleichung befindlichen Grösse abzieht von der rechten Seite der letzten Gleichung, weniger als R und mithin noch viel mehr weniger als $4q+1$ herauskommen müsse, d. h. also entweder eine negative Zahl oder eine positive

Zahl $< 4q+1$. Berechnen wir uns diesen Unterschied, so ergiebt sich derselbe gleich

$$(12)\quad \frac{15q^2}{256}+q\left(\frac{15}{4}-\frac{95k}{128}\right)-\left(\frac{81k^2}{256}+\frac{7k}{4}+1\right)+\frac{9l}{4}\left(\frac{11q-27k-64}{36}-l\right)$$

und zerfällt offenbar in zwei Partien, von denen die eine unabhängig von l ist und, in dem ungünstigsten Falle (nämlich $k=3$) und wenn man q grösser als 45 annimmt, beständig positiv und grösser als $4q$ ausfällt. Die andere Partie ist von l abhängig, verschwindet für $l=0$ und ist von da ab für alle Werthe von l unterhalb der Grenze $l=\frac{11q-27k-64}{36}$ gleichfalls positiv. Mithin besteht der Ausdruck (12) alsdann aus zwei positiven Theilen, von denen der erste schon für sich allein grösser als $4q$ ist und sein voller Werth muss daher die Grösse $4q+1$ übersteigen, was unstatthaft ist. Also alle diejenigen Zahlen von $l=4$ bis zu $l=3\frac{q-k}{8}-4$, welche unterhalb der Grenze $\frac{11q-27k-64}{36}$ sich befinden, sind mit der Ungleichung (8) unvereinbar. Das Nämliche gilt aber auch von denjenigen unter den genannten Zahlen, welche oberhalb der Grenze $\frac{11q-27k-64}{36}$ liegen.

Um dieses darzuthun bemerken wir, dass für alle solche Werthe von l die erwähnte zweite Partie in (12) negativ wird und dem absoluten Werthe nach gleichzeitig mit l wächst. Daher ist der ungünstigste Fall derjenige, wo l seinem Maximum $3\frac{q-k}{8}-4$ gleich wird. Nun geht durch diese Substitution und nach verschiedenen Reductionen der Ausdruck (12) über in

$$(13)\quad q.\left(\frac{25}{4}-k\right)+\frac{13k}{4}-19$$

d. h. in eine im Allgemeinen beständig positive Quantität. Damit dieselbe grösser als $4q$ ausfalle, ist nothwendig, wenn 1) $k=0$, dass die Ungleichung $q>8$, wenn 2) $k=1$, dass die Ungleichung $q>12$, und wenn 3) $k=12$, dass die Ungleichung $q>50$ bestehe. Wenn dagegen 4) $k=3$ ist, so ist der Ausdruck (13) nicht nothwendig grösser als $4q$, aber man kann sich wenigstens mit leichter Mühe davon überzeugen, dass er grösser wird als $4q$, sobald man den Maximalwerth von l, nämlich

$3\frac{q-k}{8}-4$, um eine einzige Einheit verkleinert. Im Allgemeinen kann daher der Ausdruck (12) in allen Fällen als positiv und grösser als $4q$ angesehen werden, sobald n zwischen den Grenzen 3 und $3\frac{q-k}{8}-3$ angenommen wird, d. h. die oben gemachte Voraussetzung ist verificirt. Daraus aber darf weiter geschlossen werden, dass die Reihe dieser Zahlenwerthe für n mit der Ungleichheit (8) sich im Widerspruche befindet, d. h. sie giebt keine Lösung der Gleichung (3), oder, was dasselbe sagt, der Gleichung (2).

2) Es sei P von der Form $4q+3$.

Wenn die Gleichung

$$(2) \quad x^2+R=(4q+1)y$$

möglich ist und x und y ihre Lösung in den kleinsten Zahlen darstellen, so ist $x<2q+1$ und $y<q+1$. Wenn nun, indem k höchstens gleich 3 sein darf, eine der Zahlen $1, 2, 3, 4, \ldots\ldots \frac{q-k}{4}+3$ für y eingesetzt die Gleichung (2) befriedigt, so geschieht dem Theoreme für den Fall $Q=1$ Genüge; ist dieses nicht der Fall, so lässt sich beweisen, dass dem Theoreme für einen der beiden Fälle entweder $Q=2$ oder $Q=3$ nothwendig genügt wird.

In der That nehmen wir an, dass die Reihe der abnehmenden Zahlen $q, q-1, \ldots\ldots q-k$ für y substituirt die Gleichung (2) gleichfalls nicht befriedigt, so lässt sich diese letztere ersetzen durch die Gleichung

$$(3) \quad (4q+3)\left(\frac{q-k}{4}+n\right)=(q+2n-\delta)^2+R,$$

wo n eine der Zahlen

$$4,\ 5,\ 6,\ 7,\ \ldots\ldots\ 3\frac{q-k}{4}$$

bezeichnet und δ eine jedenfalls nicht den Werth von n übersteigende Zahlengrösse bedeutet, und diese Gleichung gestattet die beiden folgenden Transformationen:

$$(4) \quad (4q+3)(q-k+4\delta-4n+3)=(4n-2\delta-2q-3)^2+R\,.\,2^2$$

und

$$(6) \quad (4q+3)\left(\frac{q-k}{4}+6\delta-3n-2k+3\right)=(6n-3\delta-q-3)+R\,.\,3^2$$

und, wenn (4) dem Theoreme für den Fall $Q=2$ Genüge leisten soll, so ist nothwendig und hinreichend, dass man habe

$$(5)\quad 4(n-\delta) \geqq 3\frac{q-k}{4}$$

und, wenn (6) dem Theoreme genügen soll, so ist die gleichfalls nothwendige und hinreichende Bedingung

$$(7)\quad \delta \overline{\gtrless} \frac{n}{2}+1,\quad 2n-\delta \geqq \frac{3n}{2}-1$$

und wir haben nun wieder zu zeigen, dass, wenn die Ungleichung (7) nicht besteht, d. h. wenn man hat

$$(8)\quad \delta > \frac{n}{2}+1,\quad 2n-\delta < \frac{3n}{2}-1,$$

gerade um desswillen die Ungleichung (5) bestehen muss.

Setzen wir, die Ungleichung (8) vorausgesetzt, $4(n-\delta) = 2n-4h$, so ergiebt sich aus (3), indem man R vernachlässigt, der folgende Werth für h:

$$h = \frac{3n}{2}+q-\sqrt{q^2+4qn+3n-qk+3\frac{q-k}{4}}$$

und die Ungleichung (5) wird identisch mit der folgenden

$$(10)\quad -4(q+n)+\sqrt{16q^2+64qn+48n+12(q-k)-16qk} \geqq 3\frac{q-k}{4}$$

und ihr Bestehen oder Nichtbestehen hängt von der Natur des Ausdruckes

$$(11)\quad 26qn+n(48+6k)-16n^2-\frac{105q^2}{16}+q\left(12-\frac{71k}{8}\right)-\frac{9k^2}{16}-12k$$

ab. Dieser Ausdruck braucht wiederum nur für die Reihenfolge der Werthe von n zwischen den Grenzen $3\frac{q-k}{8}-3$ und $3\frac{q-k}{4}$ betrachtet zu werden, weil die unterhalb der Grenze von $3\frac{q-k}{8}-3$ befindlichen Werthe von n mit der Ungleichung (8) unvereinbar sind. Dieses vorausgesetzt wächst er zugleich mit n und geht für den Minimumswerth dieser Grösse, nämlich $n = 3\frac{q-k}{8}-3$, über in $\frac{15q^2}{16}-q\left(\frac{95k}{8}+12\right)-\left(\frac{81k^2}{16}+84k+288\right)$ oder, wenn man diesen Ausdruck gleichfalls für den ungünstigsten Fall $k=3$ betrachtet, in $\frac{15q^2}{16}-\frac{381q}{8}-\frac{9369}{16}$. Nun aber ist diese letzte Quantität immer positiv, wenn man die Ungleichung $q > 61$ setzt; mithin gilt dasselbe noch verstärkt von dem allgemeinen Ausdruck (11), und es ist damit dargethan, dass die Ungleichungen (5) und (8) gleichzeitig bestehen.

Die Voraussetzung, auf der die letzten Schlussfolgen ruhen, ist die Unvereinbarkeit der Ungleichung (8) mit allen Werthen von n, die die Form $n = 3\,.\,\frac{q-k}{4} - l$ besitzen, wo l eine zwischen den Grenzen 3 und $3\frac{q-k}{4} - 3$ befindliche Zahl bezeichnet. Für die angegebenen Werthe von l hat man zunächst

$$q + 2n - \delta < \frac{25q}{16} - \left(\frac{9k}{16} + 1\right) - \frac{3l}{2},$$

$$(4q+3)\left(\frac{q-k}{4} + n\right) = \frac{5q^2}{2} - q\left(\frac{20k-15}{8}\right) - \frac{15q}{8} - 4ql - 3l$$

und indem man die vorhergehende Ungleichung quadrirt und von der letzten abzieht, kekommt man rechts die Differenz

$$(12)\quad \frac{15q^2}{256} + q\left(5 - \frac{95k}{128}\right) - \left(\frac{81k^2}{256} + 3k + 1\right) + \frac{9l}{4}\left(\frac{11q - 27k - 96}{36} - l\right),$$

welche, zu Folge der Gleichung (3) mit Nothwendigkeit kleiner als $4q+3$ ausfallen, also entweder eine negative Zahl oder eine positive Zahl kleiner als $4q+3$ geben muss. Dies ist nun für die in Anspruch genommenen Werthe von l eben nicht der Fall und daher waren wir vorhin berechtigt, dieselben als unverträglich mit der Ungleichung (8) in die Untersuchung nicht mit hinein zu nehmen.

In der That besteht der Ausdruck (12) aus 2 Theilen, von denen der erste unabhängig von l und, sobald man $q > 29$ annimmt, in dem ungünstigsten Falle $k = 3$ positiv und grösser als $4q+3$ ist; der zweite Theil hängt von l ab und ist von $l = 0$ bis $l = \frac{11q - 27k - 9l}{36}$ positiv. Für alle l innerhalb dieser Grenzen fällt daher der Ausdruck (12) bestimmt positiv und grösser als $4q+3$ aus, was, wie wir wissen, unstatthaft ist. Betrachten wir nun weiter den Verlauf der von l abhängigen Partie, wenn l von $l = \frac{11q - 27k - 96}{36}$ zunimmt bis $l = 3\frac{q-k}{4} - 4$, so ist sie negativ und nimmt, dem absoluten Werthe nach gleichzeitig mit l zu. Demgemäss tritt der Fall, in welchem (12) seinen kleinsten Werth erlangt, ein, wenn l seinen Maximumwerth $3\frac{q-k}{4} - 4$ erhält. Substituiren wir diesen Werth für l in (12), so ist das Endresultat

$$q\left(\frac{27}{4} - k\right) - \left(\frac{3k}{4} + 13\right),$$

d. h. eine im Allgemeinen immer positive Zahl. Diese Zahl ist für $k=0$ grösser als $4q+2$, sobald man $q>5$, für $k=1$ grösser als $4q+2$, sobald man $q>9$ und für $k=2$ grösser als $4q+2$, sobald man $q>22$ hat. Ist dagegen $k=3$, so ist sie im Allgemeinen nicht grösser als $4q+2$, aber der Ausdruck (12) würde schon für den um eine Einheit kleineren Werth $3\frac{q-k}{4}-5$ von l grösser als $4q+2$ ausfallen — und ausserdem erfordert unser Raisonnement eigentlich auch blos, dass der Ausdruck (12) überhaupt nur grösser als R ausfalle und das wird in den meisten Fällen auch für $k=3$ zutreffen.

3) Ueberblicken wir das Ganze unseres Beweises, so ist die Gültigkeit unseres Theoremes keine absolute und darf es daher kaum als eine wesentliche Bereicherung der Theorie angesehen werden. Seine Gültigkeit erscheint durchweg an gewisse Bedingungen geknüpft, die schliesslich darauf hinauslaufen, dass die Zahl q und dem zu Folge die Zahl P beträchtlich genug sei, um die Anwendung des Satzes zuzulassen. Als eine Grenze dieser Art kann im Allgemeinen die Zahl $P=250$ gelten. Indessen ist damit nicht gesagt, dass der Satz für Modul unterhalb dieser Grenze seine Anwendbarkeit verliere; dies würde ein der Natur der Sache nach nur seltenes Zusammentreffen der allerungünstigsten Bedingungen voraussetzen und selbst wenn dies eintrete, so wäre, immer vorausgesetzt dass man sich der Möglichkeit einer Lösung vorher versichert hat, nichts verloren, sondern man würde nur noch die Hinzufügung einiger neuen Versuche nöthig haben. Ausserdem ist zu bemerken, dass man Tafeln hat, welche bis zu 1000 gehen (z. B. der Canon arithmeticus) und vermöge deren die praktische Lösung irgend einer quadratischen Gleichung mit 2 Unbekannten leicht ermöglicht werden kann. Die Hauptsache für uns ist dem zu Folge, dass man für Modul, die über die Grenze der Tafeln hinausgehen, eine praktische Methode besitze und hierzu bietet allerdings der voranstehende Lehrsatz das geeignete Mittel dar.

Aus ihm folgt, dass immer eine Zahl m zwischen den Grenzen 1 und $\frac{P}{16}+3$ existirt, welche eine der Gleichungen

$$(18)\quad Pm-R.1^2=U^2,$$

$$(19)\quad Pm-R.2^2=U^2,$$

$$(20)\quad Pm-R.3^2=U^2$$

befriedigt und die Zahl der zur Ausmittelung dieses m erforderlichen Versuche kann höchstens $3\left(\frac{P}{16}+3\right)$, also ungefähr $\frac{3}{16}P$ sein. Diese Zahl m als bekannt vorausgesetzt giebt die in dem vorigen Paragraphen entwickelte Tabelle ein Mittel an die Hand, um zwei zusammengehörige Zahlenwerthe x und y zu berechnen. Zu diesem Zwecke ist indessen nicht die Benutzung der ganzen Tabelle erforderlich, sondern wir brauchen nur einen kleinen Theil derselben, nämlich folgenden:

	$R.Q^2$	$\eta = n^2+R$		
$N=1$	$R.1^2$	$n-1$	$n+1$	
$N=2$	$R.2^2$	$2n-1$	$2n+1$	$y=m\eta,\ x=2n^2\mp n+2R$
$N=3$	$R.3^2$	$3n-1$	$3n+1$	$y=m\eta,\ x=3n^2\mp n+3R$

Wir haben nun je nach der Form, welche das gefundene Vielfache Pm von P hat, 3 Fälle zu unterscheiden.

a) Das Vielfache Pm hat die Form $U^2+R.1^2$, d. h. es genügt der Gleichung (18); alsdann hat man unmittelbar eine Lösung der vorgegebenen Gleichung in x und y, nämlich $y=m$ und $x=U$.

b) Das Vielfache Pm hat die Form $U^2+R.2^2$, so dass es der Gleichung (19) genügt. Alsdann hat man die beiden Fälle, U ungerade oder gerade zu unterscheiden. In dem ersten Falle setze man U gleich einer der beiden Formen $2n-1$ oder $2n+1$ und bestimme hieraus n; alsdann ist das System der Werthe

$$y=m(n^2+R),\ x=2n^2\mp n+2R,$$

wo das obere Vorzeichen der Form $2n-1$, das untere der Form $2n+1$ entspricht, eine particuläre Lösung unserer Gleichung. In dem zweiten Falle bemerke man, dass aus der Gleichheit $P.m=U^2+R.2^2$ die andere Gleichheit $P.m'=(P-U)^2+R.2^2$ folgt, in welcher, da P als ungerade, U als gerade vorausgesetzt wird, $P-U$ ungerade ausfällt, so dass wir wieder auf den ersten Fall zurückkommen.

c) Das Vielfache Pm ist von der Form $U^2+R.3^2$, so dass es der Gleichung (20) genügt. Alsdann kann U die drei Formen $3q-1$, $3q+1$, $3q$ haben und sind hiernach drei Unterfälle zu unterscheiden. In den beiden ersten Fällen setze man, je nachdem U von der Form $3q-1$ oder

$3q+1$ ist, diese Grösse gleich $3n-1$ oder $3n+1$ und bestimme n vermöge der entstehenden Gleichung; das System der Werthe

$$y = m(n^2+R), \quad x = 3n^2 \mp n + 3R$$

giebt hierauf die gesuchte particuläre Lösung.

Im dritten Falle, wenn U von der Form $3n$ ist, muss U^2 durch 9 theilbar sein und mithin ist es auch P, so dass man $\frac{Pm}{9} = \left(\frac{U}{3}\right)^2 + R$ hat. Wenn nun P eine relative Primzahl zu 9 ist, so ist m durch 9 theilbar und das System der Werthe $x = \frac{U}{3}$, $y = \frac{m}{9}$ stellt eine particuläre Lösung unserer Gleichung dar. Ist dagegen P keine relative Primzahl zu q, so kann man immer die gegebene Gleichung auf 2 andere oder, wenn man lieber will, auf 2 Congruenzen zurückführen, deren eine zum Modul eine relative Primzahl zu 3 hat, während der Modul der anderen als irgend eine specielle Potenz von 3 sich darstellt. Will man nicht diese Zerfällung in mehrere Gleichungen anwenden, so kann man sich auch folgender Methode bedienen:

Wenn P mit 9 einen gemeinschaftlichen Theiler hat, so ist der grösste, den es mit ihm gemein hat, entweder 3 oder 9 selbst und dem entsprechend erhält man die beiden Gleichungen

$$\frac{P}{3} \cdot \frac{m}{3} = \left(\frac{U}{3}\right)^2 + R \quad \text{oder} \quad \frac{P}{9} \cdot m = \left(\frac{U}{3}\right)^2 + R.$$

Hieraus folgt nun eine particuläre Lösung der Gleichung

$$(21) \quad x^2 + R = \Pi y,$$

wo Π entweder die Bedeutung $\frac{P}{3}$ oder die Bedeutung $\frac{P}{9}$ hat. Schliesst man von der particulären Lösung nach y auf die allgemeine, so finden sich unter den darin inbegriffenen Zahlen stets solche, die respective durch 3 oder 9 ohne Rest theilbar sind. Die aus dieser Division hervorgehenden Quotienten geben Werthe von y, die sich auf die Gleichung (2) anwenden lassen. Die zugehörigen Werthe von x sind den Gleichungen (2) und (21) gemeinsam.

Die ganze Methode, die wir eben auseinandergesetzt haben, basirt auf der Möglichkeit ein solches Vielfaches von P aufzufinden, welches einer der Gleichungen (18), (19) oder (20) Genüge leistet. Für die praktische Bestimmung eines solchen Vielfachen, die immer eine Anzahl von

Versuchen erfordert, mögen folgende Bemerkungen dienen: 1) Die Zahl m ist eine der Zahlen 1, 2, 3, 4, ... $\frac{P}{16}+2$ und bleibt daher immer unterhalb der Grenze $\frac{P}{16}+3$. 2) Die Endziffer einer vollständigen ganzen Quadratzahl ist 1, 4, 6, 9, 5, 0. 3) Die Zehnerziffer einer vollständigen Quadratzahl, die auf 0 oder 5 ausgeht, ist nothwendig 0 oder 2. 4) Jede vollständige Quadratzahl, die in der Einerstelle eine 6 hat, hat in der Zehnerstelle eine ungerade Zahl. 5) Jede vollständige Quadratzahl, die in der Einerstelle mit 1, 4 oder 9 schliesst, hat in der Zehnerstelle eine ungerade Zahl.

Beispiel. $x^2+171=1559y$. Die Grenze für die m oder $\frac{P}{16}+3$ wird $97+3=100$. Bildet man sich nun zunächst die Reihe der Zahlen $P-R$, $2P-R$, $3P-R$, ... $9P-R$, so erhält man

1388 2947 4506 6065 7624 9183 10742 12301 13860 15419.

Die erste Zahl 1388 ist kein vollständiges Quadrat, weil sie auf 8 ausgeht, und damit fallen auch die Zahlen $11P-R$, $21P-R$, $31P-R$, $41P-R$, $51P-R$, $61P-R$, $71P-R$, $81P-R$, $91P-R$ aus der Betrachtung heraus, weil sie alle auf die nämliche Ziffer 8 ausgehen. Die zweite Zahl 2947 und mit ihr die Zahlen der Reihe $12P-R$, $22P-R$, ... $92P-R$ sind gleichfalls wegen der Endziffer 7 keine vollständigen Quadrate. Was ferner die Reihe der Zahlen $3P-R$, $13P-R$, $23P-R$, ... betrifft, so hat man nur diejenigen Glieder zu untersuchen, deren vorletzte Ziffer eine ungerade Zahl ist, d. h. die an den geraden Stellen sich vorfinden, nämlich

20096 51876 83056 114236 145416.

Die Ausziehung der Quadratwurzel zeigt, dass alle diese Zahlen irrational sind. Weiter in Betreff der Reihe $4P-R$, $14P-R$, ... hat man blos das einzige Glied $44P-R$ dem Versuch der Quadratwurzelausziehung zu unterwerfen, wobei ein Rest bleibt; denn die übrigen Glieder haben in der Einerstelle eine von 5 und in der Zehnerstelle eine von 2 verschiedene Zahl. Indem man in dieser Weise fortgeht, überzeugt man sich, dass den Gleichungen (18) und (19) kein Genüge geschieht. Nimmt man die dritte auf die Gleichung (20) bezügliche Versuchsreihe vor, so hat man wegen der Beschaffenheit der Einerstelle nur folgende Glieder zu berücksichtigen:

$1559.1-9.171= 20$, $1559.2-9.171=1579$, $1559.5-9.171= 6256$, $1559.6-9.171=7815$, $1559.7-9.171=9374$, $1559.10-9.171=14051$. Untersucht man nun die Reihe $P-9R$, $11P-9R$, $21P-9R$, $31P-9R$, ..., $91P-9R$ (wobei übrigens nur ein einziges Glied den Versuch einer wirklichen Quadratwurzelausziehung fordert), so findet man kein taugliches Resultat, eben so wenig ist das mit den auf 1579, 6256 und 7815 bezüglichen Versuchsreihen der Fall; dagegen die mit 9374 anfangende Zahlenreihe hat zu ihrem zweiten Gliede

$$1559.17-9.171=158^2.$$

Setzt man $3n-1=158$, so findet man $n=53$, $\eta=n^2.R=2980$, $y=m\eta=17.2980=50660$, $x=3.2809-53+513=8887$. Die gesuchte particuläre Lösung unserer Gleichung ist daher:

$$x=8887,\ y=50660.$$

Sondert man von x die Vielfachen des Moduls 1559 ab, so findet man die Lösung in den kleinsten positiven Zahlen, nämlich

$$x=\pm 467,\ y=140.$$

§. 21.

Auflösung vermöge der Methode der Ausschliessung.

Eine andere Methode, die Wurzeln der Gleichung

$$x^2+R=Py$$

aufzulösen, rührt von Gauss her; es ist die auch sonst häufig anwendbare Methode der Ausschliessung, vermöge deren solche Zahlen, die nicht fähig sind, Lösungen zu geben weggeworfen und aus der kleinen Menge der übrig bleibenden Zahlen durch Versuche diejenigen, welche Lösungen entsprechen, ausgemittelt werden.

Wir bemerken zuvörderst, dass die absoluten Zahlenwerthe von x, welche sämmtlich mögliche von einander verschiedene und in den kleinsten Zahlen ausgedrückte Lösungen geben können, nothwendig zwischen den Grenzen 0 und $\frac{P}{2}$ enthalten sind. Dadurch bekommen wir die entsprechenden Werthe der Unbestimmten y eingeschlossen zwischen den Grenzen $\frac{R}{P}$ und $\frac{1}{4}P+\frac{R}{P}$ (die, wenn R positiv und $<P$ ist, in 0 und $\frac{1}{4}P$ übergehen) und der nächst liegende Gedanke ist, wie schon im An-

fange dieses Abschnittes angedeutet wurde, in den Ausdruck $Py-R$ für y nach und nach alle zwischen diesen Grenzen befindlichen Zahlen einzusetzen und zuzusehen, wie viele unter diesen Substitutionen denselben zu einem vollständigen Quadrate machen. Wenn aber P nur einigermassen beträchtlich ist, so häuft sich die Zahl der Versuche dergestalt, dass eine Verringerung ihrer Menge äusserst wünschenswerth erscheint.

Um diesen Zweck zu erreichen, wähle man sich irgend eine ganze Zahl $E>2$ und relative Primzahl zu P; hierauf bilde man sich ihre sämmtlichen quadratischen Nichtreste, welche durch die Reihe der Zahlen $a, b, c, \ldots.$ dargestellt sein mögen, und bestimme die Zahlen $\alpha, \beta, \gamma, \ldots.$ dergestalt, dass sie in positiven Zahlen die kleinsten Lösungen der Congruenzen

$$P\alpha - R \equiv a, \quad P\beta - R \equiv b, \quad P\gamma - R \equiv c, \ \ldots\ldots \ (mod\ E)$$

ausdrücken. Alsdann kann man versichert sein, dass alle Zahlen von einer der Formen

$$Et+\alpha, \quad Et+\beta, \quad Et+\gamma, \ \ldots\ldots$$

bestimmt keine Lösungen der gegebenen Gleichung nach y sind. Denn wäre z. B. $Et+\alpha$ eine Lösung, so hätte man $x^2+R = EPt+P\alpha$, woher $x^2 \equiv P\alpha - R\ (mod\ E)$ oder $x^2 \equiv a\ (mod\ E)$, d. h. es wäre a gegen die Voraussetzung ein quadratischer Rest von E.

Beispiel. Sei die aufzulösende Gleichung

$$x^2 - 22 = 97y, \quad R = -22, \quad P = 97;$$

dann sind die Werthe von y in der Reihe der Zahlen $1, 2, 3, \ldots\ldots 24$ enthalten. Nehmen wir $E = 3$, so ist der einzige Nichtrest dazu $a = 2$ und der Congruenz $97\alpha + 22 \equiv 2\ (mod\ 3)$ geschieht Genüge durch $\alpha = 1$; mithin müssen wegen $E = 3$ alle Zahlen der Form $3t+1$ aus obiger Zahlenreihe ausgeschlossen werden. In ähnlicher Weise findet man für $E=4$ sogleich $a = 2$, $b = 3$, $\alpha = 0$, $\beta = 1$ und die beiden neuen auszuschliessenden Zahlformen $4t$ und $4t+1$. Dadurch bleiben nur noch folgende 8 Zahlen übrig: 2, 3, 6, 11, 14, 15, 18, 23. Setzen wir weiter $E = 5$, so findet man die Formen $5t$ und $5t+3$ als unzulässige und die zurückbleibenden Zahlen sind: 2, 6, 11, 14. Die Ausschliessende (wie man die Zahl E füglich bezeichnen kann) gleich 6 gesetzt giebt nichts Neues. Nimmt man endlich die Ausschliessende gleich 7, so ergeben

sich die Formen $7t+2$, $7t+3$, $7t+5$ als zu verwerfende und es bleiben noch die 3 Zahlen 6, 11, 14 übrig. Diese Zahlen in unsere Gleichung eingesetzt geben respective 604, 1089, 1380 als Werthe des Ausdruckes $Py-R$; unter denselben ist der mittlere das vollständige Quadrat von 33, mithin $x \equiv 33 \pmod{97}$.

Beispiel 2. Die aufzulösende Gleichung sei

$$x^2+37=175y,\ R=37,\ P=175=7.25.$$

$$\begin{array}{rll}
175\alpha-37 \equiv 2 \pmod{3}; & \alpha-1 \equiv 2; & \alpha=0 \\
175\beta-37 \equiv 2 & 3\beta-1 \equiv 2; & \beta=1 \\
\equiv 3 \pmod{4}; & \equiv 3; & \beta=0 \\
175\gamma-37 \equiv 2 & 7\gamma-5 \equiv 2; & \gamma=1 \\
3 & 3 & 0 \\
5 \pmod{8}; & 5 & 6 \\
6 & 6 & 5 \\
7 & 7 & 4 \\
175\delta-37 \equiv 2 & \delta+4 \equiv -2; & \delta=5 \\
6 & +5 & 1 \\
7 \pmod{11}; & +4 & 0 \\
8 & +3 & 10 \\
10 & +1 & 8
\end{array}$$

Hiernach sind wegen $E=3$ und $E=1$ folgende Formen auszuschliessen: $3t$, $4t+1$, $4t$; ferner wegen $E=8$ die Form $8t+6$ (denn die Formen $8t+1$, $8t$, $8t+5$, $8t+4$ sind in den beiden schon dagewesenen Formen $4t+1$ und $4t$ mit enthalten); endlich wegen $E=11$ die Formen: $11t+5$, $11t+1$, $11t$, $11t+10$, $11t+8$. Die Zahlenwerthe von y, um welche es sich handelt, sind zwischen den Grenzen $\frac{37}{175}$ und $\frac{175}{4}+\frac{37}{175}$, d. h. zwischen 0 und 44; schreiben wir uns daher die Zahlen von 1 bis 44 in 4 Horizontalreihen, jede zu 11 Zahlen, so fallen wegen der Formen $11t$, $11t+1$, $11t+5$, $11t+8$, $11t+10$ sogleich die 1te, 5te, 8te, 10te und 11te Verticalreihe aus und indem man durch einfaches Abzählen, ähnlich wie bei dem Siebe des Eratosthenes, die wegen der Formen $8t+6$, $4t$, $4t+1$, $3t$ überflüssigen Zahlen ausstreicht, bekommt man folgendes Schema:

~~1~~ 2 ~~3~~ ~~4~~ ~~5~~ ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ ~~11~~
~~12~~ ~~13~~ ~~14~~ ~~15~~ ~~16~~ ~~17~~ ~~18~~ ~~19~~ ~~20~~ ~~21~~ ~~22~~
~~23~~ ~~24~~ ~~25~~ 26 ~~27~~ ~~28~~ ~~29~~ ~~30~~ 31 ~~32~~ ~~33~~
~~34~~ 35 ~~36~~ ~~37~~ ~~38~~ ~~39~~ ~~40~~ ~~41~~ ~~42~~ ~~43~~ ~~44~~

und die Reihe der übrig bleibenden Zahlen ist

2 7 26 31 35.

Setzt man diese Zahlen in den Ausdruck $175y - 37$ für y ein, so wird er für keinen dieser Werthe ein vollständiges Quadrat; mithin ist die vorgegebene Gleichung überhaupt nicht möglich, oder mit anderen Worten: -37 ist ein quadratischer Nichtrest von 175. In der That kann man dieses ohne Schwierigkeit nachweisen. Denn es ist $\left(\frac{-37}{5}\right) \equiv \left(\frac{3}{5}\right) = -1$, d. h. -37 ist ein Nichtrest von 5, folgeweise auch von 25 und 175.

Fünfter Abschnitt.

Theorie der quadratischen Formen.

§. 22.

Allgemeine Erklärungen und Lehrsätze.

1) Der Ausdruck $ax^2+2bxy+cy^2$, in welchem a, b, c ganze Zahlen vorstellen, soll in dem Nachfolgenden eine quadratische Form oder auch schlechthin eine Form genannt und, wenn man wesentlich auf die Art der Abhängigkeit sieht, in welcher er von den drei constanten Grössen a, b, c steht, durch das Symbol (a, b, c) bezeichnet werden. Zugleich bemerken wir, dass die Ordnung der hierin vorkommenden Elemente a, b, c eine wesentliche Rolle spielt und demgemäss (c, b, a) eine andere quadratische Form darstellt als (a, b, c). Denken wir uns in der Form $ax^2+2bxy+cy^2$ den Grössen x und y eine specielle Bedeutung zuertheilt, so wird dieselbe irgend einen Zahlenwerth M erhalten und wir werden, um dies Verhältniss näher anzudeuten, künftig uns der Ausdrucksweise bedienen, die Zahl M werde durch die quadratische Form dargestellt oder repräsentirt. Wir werden übrigens im Nachfolgenden, wenigstens zunächst, durchweg voraussetzen, dass die speciellen Zahlenwerthe $x=m$, $y=n$, für welche eine Form die Zahl M darstellt, relative Primzahlen zu einander sind. Endlich wollen wir den Ausdruck b^2-ac, welcher für diese ganze Theorie von entscheidender Bedeutung ist, mit dem Namen der Determinanten der quadratischen Form (a, b, c) belegen und der Kürze halber durch den be-

sonderen Buchstaben D bezeichnen. In den nachfolgenden Entwickelungen ist die Determinante D durchweg als von 0 verschieden vorausgesetzt, um auf diese Weise eine grössere Concinnität in der Aussprache der Sätze zu erzielen. Nach diesen Erläuterungen gehen wir sogleich zu dem nachfolgenden Theorem über:

Wenn eine bestimmte Zahl M so durch eine gegebene Form (a, b, c) darstellbar ist, dass die Werthe der Unbestimmten x, y, für welche sich die quadratische Form auf M reducirt, relative Primzahlen zu einander sind, so ist die Determinante D ein quadratischer Rest von M.

Zu Folge der Voraussetzung ist

$$(1)\quad am^2+2bmn+cn^2=M$$

und können wir die Zahlen μ und ν auf unendlich viele Arten derartig bestimmen, dass die Gleichung

$$(2)\quad \mu m+\nu n=1$$

besteht. Wenden wir diese beiden Relationen auf die Identität

$$\left\{\mu(mb+nc)-\nu(ma+nb)\right\}^2-(b^2-ac)(\mu m+\nu n)^2=(am^2+2bmn+cn^2).(a\nu^2-2b\mu\nu+c\mu^2)$$

an, so geht dieselbe über in die Gleichung:

$$\left\{\mu(mb+nc)-\nu(ma+nb)\right\}^2-D=M(a\nu^2-2b\mu\nu+c\nu^2),$$

welche auch, indem wir

$$(3)\quad z=\mu(mb+nc)-\nu(ma+nb),\ s=a\nu^2-2b\mu\nu+c\nu^2$$

setzen, dargestellt werden kann in einer der beiden Formen

$$(4)\quad z^2-D=Ms \text{ oder } z^2\equiv D \pmod{M},$$

d. h. es ist, wie behauptet wurde, D ein quadratischer Rest von M.

Die Zahl z hängt zunächst von den Unveränderlichen m und n ab und weiter von den Zahlen μ und ν, welche sich in unendlich verschiedener Art bestimmen lassen; indessen alle irgend nur möglichen Zahlenwerthe von z, welche den verschiedenen zusammengehörigen Werthen von μ und ν entsprechen, sind einander nach dem Modul M congruent,

In der That bezeichnen μ, ν, z und μ', ν', z' zwei beliebige Systeme zusammengehöriger Werthe, so folgt zunächst aus den Gleichungen $\mu m+\nu n=1$ und $\mu'm+\nu'n=1$, dass man habe $\mu'-\mu=n(\mu'\nu-\mu\nu')$ und $\nu'-\nu=-m(\mu'\nu-\mu\nu')$, und die sich leicht ergebende Gleichung $z'-z=$,

$(\mu'-\mu)(mb+nc)-(\nu'-\nu)(ma+nb)$ gebt über in $z'-z=(\mu'\nu-\mu\nu')(am^2+2bmn+cn^2)$, woher mit Rücksicht auf (1) leicht die Congruenz $z'\equiv z$ $(mod\ M)$ erhellt.

Umgekehrt, wenn irgend eine mit z congruente Zahl z' gegeben ist, so lassen sich immer zwei solche zusammengehörige Zahlenwerthe μ', ν' bestimmen, welche an die Stelle von μ, ν substituirt die Zahl z' geben. Offenbar wird dies geleistet, indem man in den Werth von z, nämlich $\mu(mb+nc)-\nu(ma+nb)$, an Stelle von μ und ν die Zahlenwerthe $\mu'=\mu+\frac{n(z'-z)}{M}$ und $\nu'=\nu-\frac{m(z'-z)}{M}$ treten lässt; denn dadurch verwandelt er sich in $-\left\{\mu(mb+nc)-\nu(ma+nb)\right\}+\left\{\frac{z'-z}{M}(am^2+2bmn+cn^2)\right\}$; oder, da der erste Theil dieses Ausdruckes sich auf z, der zweite auf $z'-z$ reducirt in z'.

Hiernach ist es statthaft für z denjenigen Werth zu nehmen, der unter allen möglichen der kleinste ist, d. h. absolut genommen kleiner als $\frac{M}{2}$ und in diesem Sinne entspricht einer particulären Lösung der Gleichung (1) immer eine und nur eine Lösung der Congruenz (4). Die letztere wird freilich in Bezug auf z im Allgemeinen mehrere Lösungen kleiner als $\frac{M}{2}$ zulassen, aber es kann nur eine darunter die durch die erste der Gleichungen (3) vorgeschriebene Form haben, weil, wenn mehrere diese Form zu gleicher Zeit besässen, sie, wie oben gezeigt, nach dem Modul M einander congruent wären, im Widerspruche dazu, dass sie sämmtlich kleiner als $\frac{M}{2}$ sind. Also nicht jede beliebige Lösung der Congruenz (4) hat die bestimmte Lösung $x=m$, $y=n$ von (1) zu Folge oder, wenn auch, damit die Gleichung (1) in bestimmten ganzen Zahlen für x und y bestehen könne, die Bedingungscongruenz (4) nothwendig statthaben muss, so ist dies Statthaben durchaus noch kein zureichender Grund für die Existenz jener bestimmten Werthe von x und y, für welche die quadratische Form (a, b, c) die bestimmte Zahl M repräsentirt. Dieses vorausgesetzt hat es also seinen guten Sinn, wenn wir sagen, das System $x=m$, $y=n$, für welches unsere Form die bestimmte Zahl M darstellt, gehört zu der (speciellen) Lösung $z=\zeta$ der Congruenz $z^2\equiv D\ (mod\ M)$.

Wenn die Zahl M eine zweifache Darstellung durch die Form (a, b, c) gestattet, nämlich die eine entsprechend dem Systeme $x = m$ und $y = n$, die andere entsprechend dem Systeme $x = m'$ und $y = n'$, so muss sowohl das erste wie das zweite System zu irgend einer Lösung der Bedingungscongruenz

$$(5)\quad z^2 \equiv D \ (mod\ M)$$

gehören; da nun die Congruenz (5), wenn sie möglich ist, wie es hier eintreten muss, wenigstens zwei von einander verschiedene Lösungen und im Allgemeinen noch mehrere gestattet, so können hierbei folgende drei Fälle eintreten: 1) Die beiden Systeme $x = m$, $y = n$ und $x = m'$, $y = n'$ gehören zu der nämlichen Lösung von (5); 2) sie gehören zu sonst gleichen, aber einander gerade entgegengesetzten Lösungen; 3) sie gehören verschiedenen Lösungen der Congruenz (5) an, so dass dieselben, immer in der Voraussetzung, dass sie in den kleinsten Zahlen ausgedrückt sind, verschiedene absolute Werthe haben. Der Natur der Sache nach werden die nämlichen 3 Fälle eintreten können, wenn die Zahl M durch sonst verschiedene Formen, aber mit gleicher Determinante dargestellt wird; denn die Constanten der Bedingungscongruenz (5) bleiben unter dieser Voraussetzung unverändert.

Betrachten wir beispielsweise die Form

$$(3,\ 7,\ -8) = 3x^2 + 14xy - 8y^2,$$

deren Determinante den Werth 73 hat, so wird die Zahl $M = 57$ dargestellt, sowohl indem man die Werthe $x = 13$, $y = 25$, wie auch, indem man die Werthe $x = 5$, $y = 9$ einsetzt. Lösen wir die diesen beiden Systemen entsprechenden Hülfsgleichungen $13\mu + 25\nu = 1$, $5\mu' + 9\nu' = 1$ oder auch die damit identischen Congruenzen $13\mu \equiv 1$ $(mod\ 25)$, $5\mu' \equiv 1$ $(mod\ 9)$ auf, so erhalten wir $\mu = \mu' = 2$, $\nu = \nu' = -1$ und für z und z' ergeben sich jetzt vermöge (3) die Werthe:

$$z = 2(13.7 - 25.8) + (13.3 + 25.7) = -4;$$

$$z' = 2(5.7 - 9.8) + (5.3 + 9.7) = +4;$$

es tritt somit der Fall (12) ein. Uebrigens überzeugt man sich leicht, dass die Bedingungscongruenz

$$z^2 \equiv 73 \ (mod\ 57)$$

durch $z = \pm 4$ befriedigt wird. Um ihre übrigen Lösungen zu finden, bemerke man, dass sie in die beiden Congruenzen $z^2 \equiv 73$ $(mod\ 3)$ und

$z^2 \equiv 73 \ (mod\ 19)$ zerfällt, deren Lösungen respective durch die Formen $z = 3n \pm 4$ und $z = 19n' \pm 4$ dargestellt werden; offenbar sind die beiden Formen gemeinschaftlichen Zahlenwerthe die Lösungen der betrachteten Congruenz; wir erhalten dieselben daher, indem wir erstens $3n \pm 4 = 19n' \pm 4$ setzen, wodurch wir auf die schon bekannte Lösung zurückkommen, und zweitens, indem wir $3n \mp 4 = 19n' \pm 4$ setzen; dies giebt $3n = 19n' \pm 8$; $n = 6n' \pm 2 + \frac{n' \pm 2}{3}$ oder, wenn wir $n' \pm 2 = 3m$ setzen, $n = 19m \mp 10$. Hieraus folgt $z = 3n \pm 4 = 3(19m \mp 10) \mp 4 = 57m \mp 34$ oder $= 57m' \pm 23$. Dem zu Folge sind alle 4 von einander verschiedenen Lösungen unserer Congruenz in den kleinsten Zahlen

$$z \equiv +4, \ -4, \ +23, \ -23 \ (mod\ 57)$$

und man kann sich nun mit leichter Mühe direct davon überzeugen, dass die 3 letzten Lösungen mit dem Systeme $x = 13$, $y = 25$ unverträglich sind. In der That, indem man für a, b, c ihre Werthe und $m = 13$, $n = 25$ setzt, folgt das System der beiden Gleichungen

$$109\mu + 214\nu = -z, \quad 13\mu + 25\nu = 1$$

und hieraus

$$\mu = \frac{214 - 25z}{57}, \quad \nu = \frac{13z - 109}{57}.$$

Setzen wir nun für z die Lösung $+4$ ein, so bekommen wir für μ und ν, wie es sein muss, ganzzahlige Werthe; dagegen jede der 3 übrig bleibenden Lösungen $z = -4$, $+23$, -23 ergiebt für μ und ν gebrochene Zahlenwerthe. Also unter den 4 Lösungen der Bedingungscongruenz ist nur eine einzige, welche zu dem Systeme $x = 13$, $y = 25$ gehört.

2) Wenn die Form $F = (a, b, c)$, in der x, y die Unbestimmten sein mögen, durch die Substitutionen

$$(6) \quad x = \alpha x' + \beta y', \ y = \gamma x' + \delta y',$$

wo α, β, γ, δ ganze Zahlen bezeichnen, in die Form $F' = (a', b', c')$, von der die Unbestimmten x', y' sind, sich verwandelt, so sagt man, **die Form F schliesse die Form F' in sich oder die Form F' ist in der Form F enthalten.** Die Natur der Transformation wird durch die Gleichungen (6) charakterisirt und es giebt daher, da die Grössen α, β, γ, δ unendlich viele Zahlenwerthe haben können, eine unendlich grosse Menge. Je nachdem die Grösse $\alpha\delta - \beta\gamma$ wesentlich positiv oder negativ ist, heisst die **Transformation eine eigentliche oder**

uneigentliche. (Wie die Grösse $\alpha\delta-\beta\gamma$ dazu komme ein unterscheidendes Merkmal abzugeben, wird weiter unten von selbst erhellen.) Betrachten wir mehrere Transformationen unter sich, so heissen sie einander ähnlich, wenn sie alle entweder eigentliche oder alle uneigentliche sind. Es giebt also zwei Arten ähnlicher Transformation; wir werden indessen nur solche ähnliche Transformationen betrachten, die sämmtlich eigentliche sind. — Führt man die angedeuteten Substitutionen wirklich aus, so ergeben sich nach einigen Rechnungen folgende Werthe für die Constanten a', b', c':

$$(7)\quad \begin{cases} a' = a\alpha^2+2b\alpha\gamma+c\gamma^2, \quad c' = a\beta^2+2b\beta\delta+c\delta^2, \\ \qquad b' = a\alpha\beta+b(\alpha\delta+\beta\gamma)+c\gamma\delta \end{cases}$$

und daraus folgt für die Determinante der Form F'

$$(8)\quad b'^2-a'c' = (b^2-ac)(\alpha\delta-\beta\gamma)^2,$$

so dass erhellt, dass alle in der Form F enthaltenen Formen F' eine Determinante bekommen, deren Vorzeichen durch das Vorzeichen der Determinanten in der ursprünglichen Form bestimmt wird.

Aus der Betrachtung der Gleichungen (7) fliesst, dass jeder gemeinschaftliche Divisor der Zahlen a, b, c auch ein gemeinschaftlicher Divisor der Grössen a', b', c' ist, und jeder gemeinschaftliche Divisor von a, $2b$, c auch ein Divisor von a', $2b'$, c.

Die Form F geht durch die Substitution (6) in F' über. Nehmen wir nun an, dass die letztere für die speciellen Zahlenwerthe $x'=m$, $y'=n$ die Zahl M darstelle, so folgt, dass die Form F, indem man $x=\alpha m+\beta n$, $y=\gamma m+\delta n$ setzt, dieselbe Zahl M darstellen muss. Also jede Zahl, die durch die Form F' darstellbar ist, kann auch durch die Form F, in der jene enthalten ist, dargestellt werden. Wenn M auf mehrfache Weise durch die Form F' dargestellt werden kann, so wird auch die Form F eine mehrfache Darstellung der Zahl M gestatten; mithin hat M wenigstens ebenso viel von einander verschiedene Darstellungen durch die Form F wie durch die Form F'. Seien nämlich $x=m$, $y=n$ und $x'=m'$, $y'=n'$ zwei verschiedene Systeme, welche beide der Form F' den Werth M geben, so sind die auf die Form F bezüglichen Lösungssysteme, welche dieselbe Zahl geben, nämlich $x=\alpha m+\beta n$, $y=\gamma m+\delta n$ und $x=\alpha m'+\beta n'$, $y=\gamma m'+\delta n'$ gleichfalls von einander verschieden. Denn wenn man sie als

gleich annähme, so dass $\alpha m+\beta n=\alpha m'+\beta n'$ und $\gamma m+\delta n=\gamma m'+\delta n'$, so würde folgen, indem man die erste dieser Gleichungen mit δ, die zweite mit β multiplicirt und darauf subtrahirt, $(\alpha\delta-\beta\gamma)m=(\alpha\delta-\beta\gamma)m'$ und, indem man die erste mit γ, die zweite mit α multiplicirt, $(\beta\gamma-\alpha\delta)n=(\beta\gamma-\alpha\delta)n'$, d. h. es wäre gegen die Voraussetzung $m=m'$ und $n=n'$, wenigstens, wenn man, wie wir fernerhin thun werden, die Grösse $\alpha\delta-\beta\gamma$ als von 0 verschieden annimmt.

Wenn die Form F die Form F' einschliesst und die Form F' die Form F'', so schliesst die Form F auch die Form F'' ein. Seien die Unbestimmten der drei Formen F, F', F'' respective x und y, x' und y', x'' und y'' und möge F in F' übergehen durch die Substitutionen $x=\alpha x'+\beta y'$, $y=\gamma y'+\delta y'$, sowie F' in F'' durch die Substitutionen $x'=\alpha' x''+\beta' y''$, $y'=\gamma' x''+\delta' y''$; so erhellt unmittelbar, dass F in F'' übergeht durch die Substitutionen $x=\alpha(\alpha' x''+\beta' y'')+\beta(\gamma' x''+\delta' y'')$, $y=\gamma(\alpha' x''+\beta' y'')+\delta(\gamma' x''+\delta' y'')$ oder

$$x=(\alpha\alpha'+\beta\gamma')x''+(\alpha\beta'+\beta\delta')y'',\quad y=(\gamma\alpha'+\delta\gamma')x''+(\gamma\beta'+\delta\delta')y'';$$

also schliesst die Form F die Form F'' in sich. Die identische Gleichung

$$(\alpha\alpha'+\beta\gamma')(\gamma\beta'+\delta\delta')-(\alpha\beta'+\beta\delta')(\gamma\alpha'+\delta\gamma')=(\alpha\delta-\beta\gamma)(\alpha'\delta'-\beta'\gamma')$$

enthält zugleich den Beweis, dass die Determinante der Form F'' gleich $(b^2-ac)(\alpha\delta-\beta\gamma)^2(\alpha'\delta'-\beta'\gamma')^2$ ist, wie vorauszusehen war. Der vorstehende Satz lässt sich leicht verallgemeinern: Wenn eine Reihe von Formen F, F', F'', F''', ... $F^{(n)}$ gegeben ist, von denen jede die nachfolgende enthält, so enthält die erste Form gleichfalls die letzte.

Wenn die Determinanten D und D' zweier Formen F und F' einander gleich sind und zu gleicher Zeit F' unter F enthalten ist, so ist umgekehrt auch F unter F' enthalten und zwar eigentlich oder uneigentlich, je nachdem F' unter F eigentlich oder uneigentlich enthalten ist. Indem nämlich F durch die Substitutionen (6) in F' übergeht, erhellt aus der Gleichung (8), dass, wenn die beiden Determinanten gleich sein sollen, nothwendig $(\alpha\delta-\beta\gamma)^2=1$, also $\alpha\delta-\beta\gamma=$ entweder $+1$ oder gleich -1 sein muss. Entwickelt man sich nun aus (6) die Werthe von y', x', nämlich $x'=\dfrac{\delta x-\beta y}{\alpha\delta-\beta\gamma}$,

$y' = -\frac{\gamma x - \alpha y}{\alpha\delta - \beta\gamma}$: so sind dieselben zunächst ganzzahlig wegen $\alpha\delta - \beta\gamma = \pm 1$ und substituirt man sie in die Form F', nämlich in

$(a\alpha^2 + 2b\alpha\gamma + c\gamma^2)x'^2 + 2(a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta)x'y' + (a\beta^2 + 2b\beta\delta + c\delta^2)y'^2$,

so bekommt man als Nenner in jedem der 3 Glieder den Factor $(\alpha\beta - \beta\gamma)^2$, also, wenn man diesen als der Einheit gleich unterdrückt,

$$(a\alpha^2 + 2b\alpha\gamma + c\gamma^2)(\delta x - \beta y)^2 - 2\{a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta\}(\delta x - \beta y)(\gamma x - \alpha y) + (a\beta^2 + 2b\beta\delta + c\delta^2)(\gamma x - \alpha y)^2$$

und diese Form ist, wie man sich durch Entwickelung überzeugen kann, identisch mit der Form

$$(ax^2 + 2bxy + cy^2)(\alpha\delta - \beta\gamma)^2 = ax^2 + 2bxy + cy^2 = F.$$

Dass F' unter F in demselben Sinne enthalten ist, wie F unter F', erhellt aus den beiden Gleichungen

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2, \quad b^2 - ac = (b'^2 - a'c')(\alpha\delta - \beta\gamma)^2,$$

in welche die Grösse $\alpha\delta - \beta\gamma$ in vollkommen gleichmässiger Weise hineintritt.

Solche Formen, von denen jede in der anderen enthalten ist, heissen aequivalente Formen. Die Gleichheit der Determinanten ist mithin wohl nothwendig zur Aequivalenz, aber nicht hinreichend, es muss die Bedingung noch hinzutreten, dass die eine der beiden Formen in der anderen enthalten ist; denn daraus folgt, wie wir gesehen haben, auch das Umgekehrte, dass die zweite Form in der ersten enthalten ist.

Man wird in ähnlichem Sinne, wie man von einem eigentlichen und uneigentlichen Enthaltensein einer Form in einer anderen spricht, auch von einer eigentlichen und uneigentlichen Aequivalenz zweier Formen sprechen können. Wir werden aber hauptsächlich solche Formen in's Auge fassen, welche eigentlich aequivalent sind und verweisen rücksichtlich der Theorie der uneigentlich aequivalenten Formen auf die Disquisitiones arithmeticae. Also wenn wir schlechthin von aequivalenten Formen F und F' reden, so setzen wir im Allgemeinen stets die Gleichung

$$(9) \quad \alpha\delta - \beta\gamma = +1$$

voraus. Dieses vorausgesetzt lassen wir nun folgende Theoreme über aequivalente Formen folgen, welche zum Theil als unmittelbare Folgerungen aus dem Vorhergehenden des Beweises an dieser Stelle nicht bedürfen:

Theorem 1. Wenn zwei Formen einer dritten aequivalent sind, so sind sie auch unter einander aequivalent, und zwar eigentlich oder uneigentlich, je nachdem die beiden ersten Aequivalenzen in einerlei oder in verschiedenem Sinne gelten.

Theorem 2. Wenn zwei Formem F und F' aequivalent sind, so ist der grösste gemeinschaftliche Theiler der Zahlen a, b, c, oder auch der Zahlen a, $2b$, c derselbe, wie der grösste gemeinschaftliche Divisor der Zahlen a', b', c' oder auch der Zahlen a', $2b'$, c'.

Theorem 3. Die Formen $(a, -b, c)$, (c, b, a), $(c, -b, a)$ sind der Form (a, b, c) aequivalent und zwar die beiden ersten im uneigentlichen, die letzte im eigentlichen Sinne.

Um dies zu beweisen bemerke man zunächst, dass die genannten 4 Formen zunächst alle dieselbe Determinante haben. Man hat daher nur nöthig die Natur der Transformation ins Auge zu fassen, vermöge derer die letzte Form in die drei vorhergehenden übergeht. Wenden wir nach einander die Substitutionen $x = x' + 0.y'$ und $y = 0.x' - y'$, $x = 0.x' + y'$ und $y = x' + 0.y'$, $x = 0.x' - y'$ und $y = x' + 0.y'$ an, so geht die Form (a, b, c) respective über in $(a, -b, c)$, (c, b, a), $(c, -b, a)$ und der Ausdruck $\alpha\delta - \beta\gamma$ respective in $1.-1+0.0 = -1$, $0.0-1.1 = -1$, $0.0-(-1).1 = +1$, d. h. die behaupteten Aequivalenzen finden und zwar in dem angegebenen Sinne statt. Die Formen (a, b, c) und $(a, -b, c)$ heissen entgegengesetzte Formen und wir haben daher den Satz: Entgegengesetzte Formen sind einander im uneigentlichen Sinne aequivalent.

Solche quadratische Formen (a, b, c) und (c, b', c'), welche gleiche Determinanten haben und deren mittlere Coefficienten ausserdem noch der Bedingung $b + b' \equiv 0 \pmod{c}$ genügen, sollen angrenzende Formen heissen und zwar, wenn eine genauere Bezeichnung noth thun sollte, so werden wir sagen, die Form (a, b, c) in Bezug auf ihren letzten Theil ist angrenzend an die Form (c, b', c') oder auch die Form (c, b', c') in Bezug auf ihren ersten Theil ist angrenzend an die Form (a, b, c). Von Formen solcher Art gilt nun der Satz:

Theorem 4. Angrenzende Formen sind immer einander (im eigentlichen Sinne) aequivalent. Da die Gleichheit der Determinanten vorausgesetzt wird, so haben wir nur nöthig nachzuweisen, dass die Form (a, b, c) durch ganzzahlige Substitutionen in die angrenzende Form (c, b', c') übergehe und in der That wird dieses geleistet, wenn man setzt $x = 0.x' - y'$ und $y = x' + \frac{b+b'}{c}y'$ (wo $\frac{b+b'}{c}$ zu Folge der obigen Bedingungscongruenz eine ganze Zahl ist) und bemerkt, dass $c' = \frac{b'^2-(b^2-ac)}{c}$ ist. Zugleich wird der Ausdruck $\alpha\delta - \beta\gamma = 0.\frac{b+b'}{c} - (-1).1 = +1$. Uebrigens setzt dieser Beweis voraus, dass c eine von 0 verschiedene Grösse ist, weil sonst die Relation zwischen b und b' eine illusorische würde; aber dieser Fall ordnet sich dem allgemeineren unter, in welchem die Determinante D ein vollständiges Quadrat ist, und wir werden von demselben weiter unten besonders handeln.

Theorem 5. Jede von zwei aequivalenten Formen lässt ebensoviel Darstellungen einer Zahl M und nicht mehr zu, wie die andere, und die speciellen Zahlenwerthe der Veränderlichen, welche die eine Form F gleich M machen, haben denselben grössten gemeinschaftlichen Theiler, wie die entsprechenden Zahlenwerthe der Veränderlichen, welche die andere Form F' gleich M machen. Sind also die einen relative Primzahlen zu einander, so sind es auch die anderen.

Der erste Theil des Theoremes ergiebt sich daher, dass, wenn eine Form in einer anderen enthalten ist, eine Zahl M wenigstens ebensoviel Darstellungen durch die letzte gestattet, wie durch die erste; das Enthaltensein der einen Form in der anderen ist aber hier reciprok; in Folge davon muss die Anzahl der Darstellungen für beide Formen die nämliche sein. Seien ferner die speciellen Zahlenwerthe, vermöge deren F' die Zahl M darstellt, $x' = m$ und $y' = n$, so sind die speciellen Zahlenwerthe, welche der Repräsentation von M durch F entsprechen, $x = \alpha m + \beta n$ und $y = \gamma m + \delta n$. Bezeichnen wir den grössten gemeinschaftlichen Divisor von m und n durch Δ, den grössten gemeinschaftlichen Divisor von $\alpha m + \beta n$ und $\gamma m + \delta n$ dagegen durch Δ'; wählen wir hierauf

die Zahlen μ und ν derartig, dass sie die Gleichung $m\mu+n\nu=\Delta$ befriedigen (dies ist immer möglich; denn die genannte Gleichung kann auf die Form $\frac{m}{\Delta}\mu+\frac{n}{\Delta}\nu=1$ gebracht werden, wo $\frac{m}{\Delta}$ und $\frac{n}{\Delta}$ nach Voraussetzung relative Primzahlen zu einander sind) und betrachten endlich die Identität

$$(\delta\mu-\gamma\nu)(\alpha m+\beta n)-(\beta\mu-\alpha\nu)(\gamma m+\delta n)=(\alpha\delta-\beta\gamma)(m\mu+n\nu):$$

so erhellt, wegen der Relation $\alpha\delta-\beta\gamma=\pm1$, dass deren rechte Seite sich auf $\pm\Delta$ reducirt, die linke dagegen durch Δ' theilbar ist; mithin ist auch der Zahlenwerth Δ der rechten Seite durch Δ' theilbar. Nun ist aber auch umgekehrt Δ' durch Δ theilbar; denn da Δ in m und n aufgeht, so muss es in $\alpha m+\beta n$ und $\gamma m+\delta n$ und also auch in den grössten gemeinschaftlichen Divisor Δ' zwischen diesen beiden Zahlen aufgehen. Damit beide Aussagen einander nicht widersprechen, muss $\Delta=\Delta'$ sein, wie zu beweisen war.

Theorem 6. Wenn zwei aequivalente Formen dieselbe Zahl M darstellen und zwar für solche einander entsprechende Systeme der Unbestimmten, welche bezüglich durch relative Primzahlen zu einander gebildet werden, so gehören beide Systeme zu einer und derselben Lösung der Hülfsgleichung (4) $z^2-D=Ms$.

Die beiden gegebenen aequivalenten Formen seien (a, b, c) und $(a'\ b'\ c')$ und die letztere möge die erstere werden durch die Substitutionen $x'=\alpha x+\beta y$, $y'=\gamma x+\delta y$, wo die Coefficienten der Nebenbedingung $\alpha\delta-\beta\gamma=+1$ unterliegen; ferner möge M dargestellt werden durch die Form (a, b, c) vermöge der speciellen Zahlenwerthe $x=m$, $y=n$: so wird dieselbe Zahl M dargestellt durch die Form (a', b', c') vermöge der speciellen Zahlenwerthe $x'=\alpha m+\beta n$, $y'=\gamma m+\delta n$, die wir der Kürze halber durch m' und n' bezeichnen wollen. Endlich sei die zu dem Systeme $x=m$, $y=n$ gehörige Lösung der Gleichung (4) $z=\zeta$, $s=\sigma$ und die zu dem Systeme $x'=m'$, $y'=n'$ gehörige Lösung der nämlichen Gleichung $z=\zeta'$, $s=\sigma'$. Alsdann vermittelt sich der Zusammenhang der Zahlen m, n, ζ, σ, zu Folge der in der vorhergehenden Nummer enthaltenen Erörterungen, vermöge der Gleichungen

$$m\mu+n\nu=1,\ \zeta=\mu(mb+nc)-\nu(ma+nb),\ \sigma=a\nu^2-2b\mu\nu+c\mu^2$$

und der Zusammenhang der Zahlen $m' = \alpha m + \beta n$, $n' = \gamma m + \delta n$, ζ', σ' vermöge der Gleichungen

$$m'\mu' + n'\nu' = 1,\ \zeta' = \mu'(m'b' + n'c') - \nu'(m'a' + n'b'),$$
$$\sigma' = a'\nu'^2 - 2b'\mu'\nu' + c'\mu'^2.$$

Suchen wir uns jetzt zunächst die Zahlen μ' und ν' durch μ und ν auszudrücken und gehen zu dem Zwecke von der Identität

$$(\alpha m + \beta n)(\delta\mu - \gamma\nu) - (\gamma m + \delta n)(\beta\mu - \alpha\nu) = (\alpha\delta - \beta\gamma)(m\mu + n\nu)$$

aus: so lässt dieselbe, da beide Factoren rechts der Einheit gleich sind, die Gestalt $m'(\delta\mu - \gamma\nu) + n'(\alpha\nu - \beta\mu) = 1$ zu und daraus erhellt, dass die Gleichung $m'\mu' + n'\nu' = 1$ aufgelöst wird, indem man setzt:

$$\mu' = \delta\mu - \gamma\nu,\ \nu' = -(\beta\mu - \alpha\nu).$$

Die Coefficienten a, b, c, a', b', c' ferner sind zu Folge der Natur der Transformation durch die folgenden Relationen mit einander verknüpft:

$$a = a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2,\ c = a'\beta^2 + 2b'\beta\delta + c'\delta^2,$$
$$b = a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta.$$

Setzen wir jetzt in den Werth von ζ' für m', n', μ', ν' ihre Zahlenwerthe ein und ferner in den Werth von ζ für a, b, c die eben erwähnten Zahlenwerthe, so ergiebt sich nach einer Reihe von Reductionen die Gleichheit von ζ und ζ'. Aus dieser Gleichheit ergiebt sich die Gleichheit von σ und σ', weil die Relationen $\zeta^2 - D = M\sigma$, $\zeta'^2 - D = M\sigma'$ statt haben. Die Systeme $x = m$ und $y = n$, $x' = m'$ und $y' = n'$ mithin gehören zu einer und derselben Lösung der Hülfsgleichung $z^2 - D = Ms$.

Wenn demgemäss mehrere Paare von relativen Primzahlen existiren, welche Darstellungen von M durch $F = (a,\ b,\ c)$ geben und lauter verschiedenen Lösungen der Hülfsgleichung (4) zugehören, so werden die entsprechenden Systeme von Werthen der Unbestimmten in der Form F', welche dieselbe Zahl M repräsentiren, der Reihe nach den nämlichen Lösungen der Hülfsgleichung (4) zugehören; und wenn keine Darstellung von M durch die Form F möglich ist, welche zu einer bestimmten Lösung der Hülfsgleichung gehöre, so wird auch die Form F' keine Darstellung von M gestatten, welche eben dieser Lösung entsprechen könnte.

Es mag der Vollständigkeit halber noch die Bemerkung hinzugefügt werden, dass, wenn die beiden Formen F und F' im uneigentlichen Sinne aequivalent sind, die beiden einander entsprechenden Systeme m und n,

m' und n' zu sonst gleichen, aber einander entgegengesetzten Lösungen der Hülfsgleichung (4) gehören.

Theorem 7. Wenn das System der Zahlen $x=m$, $y=n$ (die keinen gemeinschaftlichen Theiler besitzen) einer Darstellung der Zahl M durch die Form F entspricht und die dazu gehörige Lösung der Hülfsgleichung (4) $z=\zeta$ und $s=\sigma$ ist, so sind die beiden Formen (a, b, c) und (M, ζ, σ) einander (im eigentlichen Sinne) aequivalent.

Zunächst sind die beiden Determinanten b^2-ac und $\zeta^2-M\sigma$ einander gleich wegen der Gleichungen $b^2-ac=D$ und $\zeta^2-D=M\sigma$. Indem wir daher in die Form (a, b, c) die Substitutionen $x=mx'-\nu y'$, $y=nx'+\mu y'$ einsetzen und hierin die Grössen μ und ν vermöge der bekannten Hülfsgleichung $m\mu+n\nu=1$ bestimmen, so dass durch diese Nebenbedingung die Transformation als eine eigentliche sich charakterisirt, haben wir zuzusehen, ob die auf diese Weise hervorgehenden neuen Coefficienten den Bedingungen

$$M=am^2+2bmn+cn^2,\quad \sigma=a\nu^2-2b\nu\mu+c\mu^2,$$
$$\zeta=-am\nu+b(m\mu-n\nu)+cn\mu$$

(dieselben ergeben sich aus der Gleichung (7), indem man $\alpha=m$, $\beta=-\nu$, $\gamma=n$, $\delta=\mu$ annimmt) Genüge leisten. Die erste wird erfüllt, weil die Zahl M durch die Form F vermöge der Zahlenwerthe $x=m$, $y=n$ dargestellt wird; die dritte und zweite ist identisch mit den beiden Gleichungen (3), wenn man erwägt, dass die Grössen σ und ζ hier genau die nämliche Rolle spielen, wie dort die Grössen s und z.

Betrachten wir beispielsweise die Form $3x^2+2xy+4y^2$, so ist $M=188$, wenn man einsetzt $x=4$, $y=5$; es wird ferner $4\mu+5\nu=1$, also $\mu=-1$, $\nu=1$, $z=-(4+20)-(12+5)=-41$. Die dem Systeme $x=4$, $y=5$ zugehörige Lösung der Hülfsgleichung $z^2+11=188s$ wird daher $z=-41$, $s=9$ und die Formen $3x^2+2xy+4y^2$ und $188x'^2-82x'y'+9y'^2$ sind dem zu Folge einander aequivalent. Von der Gleichheit der beiden Determinanten überzeugt man sich leicht und die Transformation, vermöge deren die erste in die letzte übergeht, ist $x=4x'-y'$, $y=5x'-y'$. Die umgekehrte Transformation ist $x'=y-x$, $y'=4y-5x$.

Theorem 8. Zwei nicht aequivalente Formen von einerlei Determinante können nicht dieselbe Primzahl darstellen.

Zunächst kann man leicht nachweisen, dass die Werthe der Unbestimmten, für welche eine Form die Primzahl M darstellt, nothwendig relative Primzahlen zu einander sind. Denn hätten sie einen von 1 verschiedenen Factor mit einander gemein, so müsste das Quadrat desselben ein Theiler von M sein, was nicht angeht. Dies vorausgesetzt sei M dargestellt durch jede der beiden Formen F und F' und zwar indem die Unbestimmten respective die Werthe m, n und m', n' erhalten. Diese beiden Werthsysteme müssen nun nothwendig entweder zu derselben oder zu gerade entgegengesetzten Lösungen der Hülfscongruenz (5) gehören. Denn da M als absolute Primzahl vorausgesetzt wird, so existiren nur 2 Lösungen, die, in den kleinsten Zahlen ausgedrückt, einander gerade entgegengesetzt sind. Die entsprechenden Lösungen der Hülfsgleichung (4) sind $z = +\zeta$, $s = \sigma$ und $z = -\zeta$, $s = \sigma$ und wir haben daher nach dem vorhergehenden Theoreme, je nachdem die Systeme m, n und m', n' gleichen oder entgegengesetzten Lösungen der Hülfsgleichung (4) zugehören, die beiden Formen F und F' entweder aequivalent der nämlichen Form $(M, \pm\zeta, \sigma)$ oder aber sie sind bezüglich den entgegengesetzten Formen $(M, \pm\zeta, \sigma)$ und $(M, \mp\zeta, \sigma)$ aequivalent. Im ersten Falle erhellt unmittelbar nach Theorem 1) die Aequivalenz der beiden Formen F und F' im eigentlichen Sinne, im zweiten Falle dagegen erhellt sie als im uneigentlichen Sinne stattfindend, wenn man bemerkt, dass entgegengesetzte Formen einander im uneigentlichen Sinne aequivalent sind und darauf wieder das Theorem 1) anwendet.

Wenn hiernach zwei Formen mit derselben Determinante D die nämliche Primzahl darstellen, so sind sie jedenfalls aequivalent. Sind sie also nicht aequivalent, so werden die Primzahlen, welche die eine etwa darzustellen fähig ist, auch nur durch sie allein oder die ihr aequivalenten Formen dargestellt und es ist nicht möglich irgend eine von ihnen durch die andere Form darzustellen.

3) Sehen wir, um uns zu orientiren, zu, warum es sich hauptsächlich handelt und in welchem Verhältnisse hierzu die vorhergehenden Entwickelungen stehen, so ist der Zweck unserer Untersuchung zu erforschen, in wiefern eine Form von gegebener Zusammensetzung eine gegebene Zahl darstellen könne oder nicht, d. h. mit anderen Worten, ob die Gleichung

$$ax^2+2bxy^2+cy=M$$

in ganzen Zahlen für x und y aufgelöst werden könne oder nicht. Dies Problem wird durch das Theorem 7) auf das andere zurückgeführt, eine gegebene Form F in eine andere von gegebener Zusammensetzung zu transformiren. Ist nämlich unsere Gleichung möglich, so existiren immer solche der Hülfsgleichung (4) genügende Werthe von z und s, nämlich $z=\zeta$ und $s=\sigma$, vermöge deren die Form (M, ζ, σ) gebildet werden kann, welche der gegebenen aequivalent ist und aus derselben vermöge der Substitutionsformeln $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$ folgt. Gemäss dem Beweise von Theorem 7) stellen alsdann die beiden Coefficienten von x' eine Lösung der gegebenen Gleichung dar, nämlich $x=\alpha$, $y=\gamma$.

Wir haben also eine doppelte Aufgabe zu erledigen, einmal, da die Congruenz (4), welche die speciellen Werthe von ζ und σ liefert, im Allgemeinen mehrere Auflösungen zulässt, diejenige unter den möglichen Formen (M, ζ, σ) herauszuwählen, in welcher die ζ und σ einem Lösungssysteme der vorgegebenen Gleichung zugehören, und dann weiter, wenn die Form (M, ζ, σ) bestimmt ist, die Transformationsformeln von F in $F'=(M, \zeta, \sigma)$ aufzustellen. Indessen wird es von jetzt ab nothwendig die Untersuchung für die drei verschiedenen möglichen Fälle 1) die Determinante D ist negativ, 2) die Determinante D ist positiv und keine Quadratzahl, 3) die Determinante D ist positiv und eine Quadratzahl, abgesondert zu führen und nur die Lösung einer Aufgabe, welche die Transformation betrifft, möge an dieser Stelle noch einen Platz finden, weil sie von der Natur der Determinanten unabhängig ist.

Es sei die Reihe der Formen F, F', F'', F''', ... $F^{(n)}$ gegeben, von denen jede in Bezug auf ihre letzte Partie der nachfolgenden angrenzend ist: man soll die Transformation der ersten in die letzte finden. Indem wir diese Formen, wie folgt, darstellen: (a, b, a'), (a', b', a''), (a'', b'', a'''), ... $(a^{(n)}, b^{(n)}, a^{(n+1)})$ und ihre Unbestimmten respective durch x und y, x' und y', x'' und y'', ... $x^{(n)}$ und $y^{(n)}$ bezeichnen, müssen die Gleichungen bestehen:

$$\frac{b+b'}{a'}=h', \quad \frac{b'+b''}{a''}=h'', \quad \frac{b''+b'''}{a'''}=h''', \quad \ldots\ldots \quad \frac{b^{(n-1)}+b^{(n)}}{a^{(n)}}=h^{(n)}$$

und man hat die Transformationsformeln

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y',$$
$$x = \alpha'' x'' + \beta'' y'', \quad y = \gamma'' x'' + \delta'' y'',$$
$$x = \alpha''' x''' + \beta''' y''', \quad y = \gamma''' x''' + \delta''' y''',$$

. . . .

. . . .

$$x = \alpha^{(n)} x^{(n)} + \beta^{(n)} y^{(n)}, \quad y = \gamma^{(n)} x^{(n)} + \delta^{(n)} y^{(n)}.$$

Diese Gleichungen stehen unter der allgemeinen Form $x = \alpha^{(m)} x^{(m)} + \beta^{(m)} y^{(m)}$, $y = \gamma^{(m)} x^{(m)} + \delta^{(m)} y^{(m)}$ und, wenn man hierin die Substitutionen einsetzt, vermöge derer $F^{(m)}$ in die angrenzende Form $F^{(m+1)}$ übergeht (vergl. Theorem 4)), nämlich $x^{(m)} = -y^{(m+1)}$, $y^{(m)} = x^{(m+1)} + k^{(m+1)} y^{(m+1)}$, so resultiren die beiden allgemeinen Formeln:

$$x = \beta^{(m)} x^{(m+1)} + (\beta^{(m)} k^{(m+1)} - \alpha^{(m)}) y^{(m+1)},$$
$$y = \delta^{(m)} x^{(m+1)} + (\delta^{(m)} k^{(m+1)} - \gamma^{(m)}) y^{(m+1)},$$

welche Geltung haben für die Werthe $m = 1, 2, 3, 4, \ldots\ldots (n-1)$. Indem man diese Werthe wirklich einsetzt, folgen der Reihe nach die Gleichungen:

$$\begin{array}{llll}
\alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = k' \\
\alpha'' = \beta' & \beta'' = \beta' k'' - \alpha' & \gamma'' = \delta' & \delta'' = \delta' k'' - \gamma' \\
\alpha''' = \beta'' & \beta''' = \beta'' k''' - \alpha'' & \gamma''' = \delta'' & \delta''' = \delta'' k''' - \gamma'' \\
\alpha^{IV} = \beta''' & \beta^{IV} = \beta''' k^{IV} - \alpha''' & \gamma^{IV} = \delta''' & \delta^{IV} = \delta''' k^{IV} - \gamma'''
\end{array}$$

. . . .

. . . .

$$\alpha^{(n)} = \alpha^{(n-1)} \quad \beta^{(n)} = \beta^{(n-1)} k^{(n)} - \alpha^{(n-1)} \quad \gamma^{(n)} = \delta^{(n-1)} \quad \delta^{(n)} = \delta^{(n-1)} k^{(n)} - \gamma^{(n-1)}.$$

Hieraus ergiebt sich weiter:

$$\begin{array}{llll}
\alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = k' \\
\alpha'' = \beta' & \beta'' = k'' \beta' & \gamma' = \delta' & \delta'' = k'' \delta' - 1 \\
\alpha''' = \beta'' & \beta''' = k''' \beta'' - \beta' & \gamma''' = \delta'' & \delta''' = k''' \delta'' - \delta' \\
\alpha^{IV} = \beta''' & \beta^{IV} = k^{IV} \beta''' - \beta'' & \gamma^{IV} = \delta''' & \delta^{IV} = k^{IV} \delta''' - \delta''
\end{array}$$

. . . .

. . . .

$$\alpha^{(n)} = \beta^{(n-1)} \quad \beta^{(n)} = k^{(n)} \beta^{(n-1)} - \beta^{(n-2)} \quad \gamma^{(n)} = \delta^{(n-1)} \quad \delta^{(n)} = k^{(n)} \delta^{(n-1)} - \delta^{(n-2)}$$

und können zu Folge dieser Formeln die Grössen $\alpha^{(n)}$, $\beta^{(n)}$, $\gamma^{(n)}$, $\delta^{(n)}$ auf recurrirendem Wege allmälig berechnet werden. Der Algorithmus, vermöge dessen das geschieht, ist ähnlich dem Algorithmus, welcher bei

der Berechnung der Näherungsbrüche zu einem Kettenbruche angewandt wird und kann in folgender Weise schematisch dargestellt werden:

		h'	h''	h'''	h^{IV}
(X)	0	-1	$-h''$	$-h'''h''+h'$	$-h^{IV}h'''h''+h'''+h''$
(Y)	1	h'	$h''h'-1$	$h'''h''h'-h'''-h'$	$h^{IV}h'''h''h'-h^{IV}h'''-h^{IV}h'-h''h'+1$

Die Grössen h', h'', h''', ..., die sich ihrer Entstehung nach als Resultate ausgeführter Divisionen ausweisen, mögen kurzweg als erster, zweiter, dritter .... Partialquotient bezeichnet werden: dann hat man folgende Regel, vermöge deren mit Ausschluss des ersten und zweiten Gliedes alle Glieder sowohl der Reihe X, wie der Reihe Y der Reihe nach sich bilden lassen: Um irgend ein Glied der Reihe X oder Y zu bilden, multiplicire man den bezüglichen Partialquotienten in das erstvorhergehende Glied und subtrahire von dem Producte das zweitvorhergehende Glied. Der Beweis ist leicht aus den obigen Formeln zu entnehmen und mag daher übergangen werden. Wenn auf diese Weise die beiden Reihen X und Y gebildet sind, so liefert uns die erste die Coefficienten der auf x, und die zweite die Coefficienten der auf y bezüglichen Substitution, vermöge derer die Form F in irgend eine Form $F^{(m)}$ übergeht. Indem wir nämlich $x=\alpha^{(m)}x^{(m)}+\beta^{(m)}y^{(m)}$ und $y=\gamma^{(m)}x^{(m)}+\delta^{(m)}y^{(m)}$ haben, sind $\beta^{(m)}$ und $\delta^{(m)}$ die auf den Partialquotienten $h^{(m)}$ bezüglichen Glieder der beiden Reihen (X) und (Y), und $\alpha^{(m)}$ und $\gamma^{(m)}$ sind die auf den vorhergehenden Partialquotienten $h^{(m-1)}$ bezüglichen Glieder.

Damit die Entwickelung der beiden Reihen X und Y möglich sei, müssen die Quotienten h', h'', h''', ... nothwendig alle endliche Zahlenwerthe haben; dies ist immer der Fall, wenn keiner der Coefficienten a', a'', a''', a^{IV}, ... $a^{(n)}$ der 0 gleich ist.

Beispiel. Gegeben seien die Formen

$$F=(23,\ 38,\ 63),\ F'=(63,\ 25,\ 10),\ F''=(10,\ 5,\ 3),\ F'''=(3,\ 1,\ 2),$$
$$F^{IV}=(2,\ -7,\ 27),\ F^{V}=(27,\ -20,\ 15),\ F^{VI}=(15,\ 20,\ 27),$$

welche alle dieselbe negative Determinante -5 besitzen, alsdann hat man

$$h'=\frac{38+25}{63}=+1,\ h''=\frac{25+5}{10}=3,\ h'''=\frac{5+1}{3}=2,\ h^{IV}=\frac{1-7}{2}=-3,$$
$$h^{V}=\frac{-7-20}{27}=-1,\ h^{VI}=0$$

und die Berechnung des obigen Schemas führt sich wie folgt aus:

		1	3	2	—3	—1	0
(X)	0	—1	—3	—5	18	—13	—18
(Y)	1	1	2	3	—11	8	11

und hiernach geht F in F^{VI} über, wenn man setzt

$$x = -13x^{VI} - 18y^{VI}, \quad y = 8x^{VI} + 11y^{VI};$$

es geht ferner F in F''' über durch Anwendung der Transformation $x = -3x''' - 5y'''$, $y = 2x''' + 3y'''$.

Betrachten wir die Bedingungen näher, denen unsere Reihe angrenzender Formen genügen muss, so finden sich dieselben ausgesprochen in den beiden Gleichungssystemen:

$$b^2 - aa' = b'^2 - a'a'' = b''^2 - a''a''' = b'''^2 - a'''a^{IV} = \ldots\ldots$$

$$b + b' = a'h'; \; b' + b'' = a''h''; \; b'' + b''' = a'''h'''; \; \ldots\ldots$$

Dieselben zeigen, dass man, wenn die erste Form F gegeben ist, man die übrigen Formen F', F'', F''', ... sich in folgender Weise herleiten kann. Man löse zuerst die Gleichung $b + b' = a'h''$ nach den beiden darin vorkommenden Unbestimmten b' und h' auf. Nun ist $b^2 - aa' = b'^2 - a'a''$, also folgt nach einander $b^2 - b'^2 = aa' - a'a''$, $(b+b')(b-b') = a'(a-a'')$, $a'h'(b-b') = a'(a-a'')$ und endlich, wenn man mit a' hebt und a'' entwickelt, $a'' = a - h'(b-b')$. Ganz ebenso entwickelt man sich $a''' = a' - h''(b'-b'')$, $a^{IV} = a'' - h'''(b''-b''')$ u. s. w.; mithin können die beiden eben genannten Gleichungssysteme auch durch die nachfolgenden Gleichungen ersetzt werden:

$$(A) \left\{ \begin{array}{ll} b + b' = a'h', & a'' = a - h'(b - b'), \\ b' + b'' = a''h'', & a''' = a' - h''(b' - b''), \\ b'' + b''' = a'''h''', & a^{IV} = a'' - h'''(b'' - b'''), \\ \ldots\ldots\ldots\ldots & \\ \ldots\ldots\ldots\ldots & \\ b^{(n-2)} + b^{(n-1)} = a^{(n-1)}h^{(n-1)}, & a^{(n)} = a^{(n-2)} - h^{(n-1)}(b^{(n-2)} - b^{(n-1)}). \end{array} \right.$$

Indem die erste Gleichung jeder Horizontalreihe immer zwei Unbestimmte (z. B. in der ersten sind es b' und h', in der zweiten b'' und h'', in der dritten b''' und h''' u. s. w.) enthält, welche eine unendlich mannigfaltige Bestimmung zulassen, die zweite Gleichung dagegen immer für jedes System von zusammengehörigen Werthen dieser Unbestimmten nach einander

die Coefficienten a'', a''', a^{IV}, ... in unzweideutiger und endlicher Weise bestimmt: ergeben sich unendlich viele von einander verschiedene Reihen angrenzender Formen, die alle mit der Form (a, b, a') als erster beginnen. Unter diesen Reihen wird sich besonders diejenige hervorheben, welche lauter Lösungen der verschiedenen unbestimmten Gleichungen in den kleinsten Zahlen entspricht und wir werden sogleich im nächsten Paragraphen auf die Betrachtung dieser Reihe näher eingehen.

§. 23.

Von den quadratischen Formen mit negativer Determinante.

1) Indem wir in diesem Paragraphen nur solche quadratische Formen, wie $F = (a, b, c)$, betrachten, deren Determinante wesentlich negativ, also von der Form $-D$ ist, so dass man $D = ac - b^2$ als eine wesentlich positive Grösse hat: ergiebt sich, dass a und c beide von demselben Zeichen, also beide entweder positiv oder negativ sein müssen. Zugleich erhellt, dass, wenn a und c positiv sind, die Form $(a, b, c) = ax^2 + 2bxy + cy^2$ für alle möglichen Werthe von x und y nur positive Zahlen M darstellen kann; denn aus der Ungleichung $ac > b^2$ folgt $a > \frac{b^2}{c}$ und, wenn man in der Form (a, b, c) für a den kleinern Werth $\frac{b^2}{c}$ substituirt, so geht sie über in $\frac{b^2}{c}x^2 + 2bxy + cy^2 = \frac{(bx+cy)^2}{c}$, d. h. in eine unter allen Umständen positive Zahl. In Folge hiervon wird unsere Form, wenn a und c beide negative Zahlen sind, nur negative Zahlen M darstellen können und man wird diesen Fall auf den vorigen zurückführen können, wenn man statt der Form F die Form $-F$ betrachtet, in welcher a und c beide positiv sein werden. Es ist daher allgemein statthaft, nur solche Formen $F = (a, b, c)$ zu betrachten, in denen die Coefficienten a und c beide positiv sind. Wir bemerken noch, dass nur ein einziges System von Werthen der x und y existirt, für welches die Form gleich 0 wird, nämlich $x = 0$, $y = 0$. Denn wenn man sie mit a multiplicirt und dem Producte die Form $(ax + by)^2 + Dy^2$ giebt, so sind beide Glieder dieser Summe wesentlich

positiv und sie kann sich daher nur so annulliren, dass man $y = 0$, $cx + by = 0$ setzt, woraus $y = 0$, $x = 0$ folgt.

Nehmen wir jetzt wieder die Betrachtung der Reihe von angrenzenden Formen:

$$(a, b, a'), (a', b', a''), (a'', b'', a'''), \ldots\ldots (a^{(n-1)}, b^{(n-1)}, c^{(n)})$$

auf, so erhellt sofort, dass alle die Grössen $a, a', a'', a''', \ldots\ldots a^{(n)}$ positiv sein müssen. Denn a und a' sind es als Coefficienten der Ausgangsform. Weil nun in der zweiten Form, die ja dieselbe negative Determinante, wie die erste, hat, a' und a'' dasselbe Zeichen haben müssen und a' positiv ist, so muss es auch a'' sein und das geht so weiter fort. Schreiben wir uns ferner die Gleichungen $b + b' = a'h'$, $b' + b'' = a''h''$, ... in dem Gleichungssystem (A) des vorigen Paragraphen, wie folgt, um: $b' \equiv -b \pmod{a'}$, $b'' \equiv -b' \pmod{a''}$, ..., so ergiebt sich sofort, dass, wenn man diese Congruenzen sich in den kleinsten Zahlen auflöst, den absoluten Werthen nach mit Nothwendigkeit die Umgleichungen

$$b' \overset{=}{<} \tfrac{1}{2}a', \quad b'' \overset{=}{<} \tfrac{1}{2}a'', \quad b''' \overset{=}{<} \tfrac{1}{2}a''', \ldots\ldots b^{(n-1)} \overset{=}{<} \tfrac{1}{2}a^{(n-1)}$$

bestehen.

Endlich, da die Zahlen $a, a', a'', a''', \ldots\ldots$ alle positiv sind, folgt aus der Betrachtung der Ausdrücke für $a'', a''', a^{IV}, \ldots\ldots$ in demselben Gleichungssysteme (A), dass, wenn die Reihe nur weit genug fortgesetzt wird, man habe

$$a'' < a, \quad a''' < a', \quad a^{IV} < a'', \quad a^{V} < a''', \ldots\ldots a^{(n)} = a^{(n-2)}.$$

Betrachten wir, um dieses nachzuweisen, die beiden allgemeinen Gleichungen

$$b^{(m-2)} + b^{(m-1)} = a^{(m-1)}h^{(m-1)}, \quad a^{(m)} = a^{(m-2)} - h^{(m-1)}(b^{(m-2)} - b^{(m-1)}),$$

so folgt aus der ersten, dass der Ausdruck $h^{(m-1)}(b^{(m-2)} - b^{(m-1)})$ keinesfalls negativ sein kann. Denn es wird zu Folge derselben der in Frage stehende Ausdruck gleich $a^{(m-1)}h^{(m-1)2} - 2b^{(m-1)}h^{(m-1)}$ und dieser letztere Ausdruck kann nicht negativ werden, weil der absolute Werth von $b^{(m-1)} \overset{=}{<} \tfrac{1}{2}a^{(m-1)}$ und mithin $a^{(m-1)}h^{(m-1)2} - 2b^{(m-1)}h^{(m-1)} \geqq a^{(m-1)}h^{(m-1)2} - a^{(m-1)}h^{(m-1)}$ ist. Dies vorausgesetzt erhellt aus der zweiten Gleichung, dass $a^{(m)} \leqq a^{(m-2)}$ ist (die Gleichheit wird eintreten, wenn man $b^{(m-1)} = \tfrac{1}{2}a^{(m-1)}$ und $h^{(m-1)} = \pm 1$ hat).

Nehmen wir weiter an, indem wir die Zahl m nach und nach die Werthe 1, 2, 3, 4, ... durchlaufen lassen, der specielle Werth $m = n$ sei der erste, für welchen die eben bewiesene Ungleichung $a^{(m)} \leqq a^{(m-2)}$ in die Gleichung $a^{(n)} = a^{(n-2)}$ übergeht: dann sind die beiden Formen $(a^{(n-2)}, b^{(n-2)}, a^{(n-1)})$ und $(a^{(n-1)}, b^{(n-1)}, a^{(n)})$ als angrenzende Formen einander eigentlich aequivalent, also müssen die beiden Determinanten gleich sein und das ist wegen der angenommenen Gleichheit zwischen $a^{(n)}$ und $a^{(n-2)}$ nur möglich, wenn die mittleren Coefficienten $b^{(n-2)}$ und $b^{(n-1)}$ gleiche absolute Werthe haben. Betrachten wir die Vorzeichen dieser beiden Coefficienten, so müssen dieselben, da die Aequivalenz im eigentlichen Sinne statthaben soll, zu Folge des Theoremes 3) im vorigen Paragraphen, entgegengesetzt sein, also $b^{(n-1)} = -b^{(n-2)}$. Wollte man nun die Reihe noch weiter fortsetzen, so würde aus der Gleichung $b^{(n-1)} + b^{(n)} = a^{(n)}h^{(n)}$ oder auch $-b^{(n-2)} + b^{(n)} = a^{(n-2)}h^{(n)}$ sich als Lösung in den kleinsten Zahlen $b^{(n)} = b^{(n-2)}$, $h^{(n)} = 0$ ergeben, woher weiter $a^{(n+1)} = a^{(n-1)}$ folgen würde. Die nächstfolgende Form wäre daher $(a^{(n-2)}, b^{(n-2)}, a^{(n-1)})$, d. h. sie fiele mit einer schon früher dagewesenen zusammen. Also, wenn die Gleichheit $a^{(n)} = a^{(n-2)}$ eintritt, so liefert die Fortsetzung der Reihe nichts Neues, sondern nur die beständige Wiederholung der beiden zuletzt erhaltenen Formen $(a^{(n-2)}, b^{(n-2)}, a^{(n-1)})$ und $(a^{(n-1)}, b^{(n-1)}, a^{(n)})$, und wir brechen sie daher bei der ersten derartigen Gleichung ab.

Nun muss diese Gleichung irgend einmal eintreten und mithin die Reihe, in dem oben bezeichneten Sinne, zum Abschlusse kommen. Denn aus den oben bewiesenen Ungleichungen schliessen wir

$$a > a'' > a^{IV} > a^{VI} > \ldots\ldots \text{ und } a' > a''' > a^{V} > a^{VII} > \ldots\ldots,$$

d. h. die Coefficienten a nehmen mit wachsenden Indices ab. Da sie nun stets ganze positive Zahlen, so ist die endliche Grenze für die Abnahme, wenn sie nicht schon früher eintreten sollte, entweder 0 oder 1. Nun kann $a^{(n)}$ nicht 0 werden, weil sonst die Determinante der letzten Form $(a^{(n-1)}, b^{(n-1)}, a^{(n)})$ gegen die Voraussetzung positiv wäre, also bleibt nur die Annahme $a^{(n)} = 1$ übrig, welche, da $a^{(n-2)}$ eine ganze Zahl ist, die Gleichung $a^{(n)} = a^{(n-2)}$ zu Folge hat. Also wird die vorangestellte Reihe von Ungleichungen

$$a'' < a, \; a''' < a', \; a^{IV} < a'', \; \ldots\ldots \; a^{(n)} = a^{(n-2)}$$

nothwendig mit einer Gleichung schliessen und zwar spätestens, wenn $a^{(n)}$

den Werth 1 erlangt, möglicher Weise aber auch schon vorher, wenn $a^{(n)}$ einen höheren Werth als 1 hat.

Die beiden Formen, mit denen unsere Reihe hiernach schliesst, sind $(a^{(n-2)}, b^{(n-2)}, a^{(n-1)})$ und $(a^{(n-1)}, -b^{(n-2)}, a^{(n-2)})$. Sehen wir uns dieselben näher an, so kann der absolute Werth des mittleren Coefficienten $\pm b^{(n-2)}$, wie oben gezeigt ist, in keinem Falle die Hälfte des ersten Coefficienten übersteigen, mag man nun die erste oder die zweite Form nehmen. Was ferner die beiden äusseren Coefficienten anbetrifft, so stehen sie entweder in dem Verhältnisse der Gleichheit oder Ungleichheit, und da, wenn letzteres eintritt, das Verhältniss der Ungleichheit in beiden Formen ein verschiedenes ist, so folgt, dass in irgend einer von beiden der dritte Coefficient entweder gleich dem ersten oder grösser als der erste sein muss. Sei diese Form (A, B, C), so hat man $D = AC - B^2$, also, wenn man C durch die jedenfalls nicht grössere Zahl A und B durch die jedenfalls nicht kleinere Zahl $\frac{1}{2}A$ ersetzt, $D \overline{\overline{<}} A^2 - \frac{1}{4}A^2$, woher $A \overline{\overline{<}} \sqrt{\frac{4}{3}D}$. Eine solche Form von der Beschaffenheit, wie die eben bezeichnete, heisst eine reducirte Form und wir können daher die Merkmale, die eine solche constituiren, in folgender Weise zusammenfassen:

Eine reducirte Form (A, B, C) ist eine solche, in welcher der dritte Coefficient nicht kleiner als der erste und der zweite Coefficient (absolut genommen) nicht grösser als die Hälfte des ersten ist. Der erste Coefficient A einer reducirten Form darf nicht mehr als $\sqrt{\frac{4}{3}D}$ betragen.

Wie man zu einer gegebenen Form die reducirte, die ihr aequivalent ist, finde, erhellt aus dem Vorstehenden; wir wollen indessen zur Verdeutlichung des Verfahrens ein Beispiel durchführen. Sei die gegebene Form $304x^2 + 434xy + 155y^2$, so lässt sich die Rechnung auf folgendes Schema bringen:

$(a, b, a') = (304, 217, 155)$; $217 + b' = 155h'$, $h' = 1$, $b' = -62$, $a'' = 304 - (217 + 62) = 25$;

$(a', b', a'') = (155, -62, 25)$; $-62 + b'' = 25h''$, $h'' = -2$, $b'' = 12$, $a''' = 155 + 2(-62 - 12) = 7$;

$(a'', b'', a''') = (25, 12, 7)$; $12 + b''' = 7h'''$, $h''' = 2$, $b''' = 2$, $a^{IV} = 25 - 2(12 - 2) = 5$;

$(a''', b''', a^{IV}) = (7, 2, 5)$; $2 + b^{IV} = 5h^{IV}$, $h^{IV} = 0$, $b^{IV} = -2$, $a^{V} = 7 - 0.(7 - 5) = 7 = a'''$;

$(a^{IV}, b^{IV}, a^{V}) = (5, -2, 7)$.

Die Reihe der angrenzenden Formen ist daher:
(304, 217, 155), (155, —62, 25), (25, 12, 7), (7, 2, 5), (5, —2, 7) und unter den beiden letzten ist es die letzte, welche in reducirter Gestalt auftritt. Die Transformation, vermöge deren (304, 217, 155) in die reducirte Form (5, —2, 7) übergeht, ist $x = 5x^{IV} - 2y^{IV}$, $y = -7x^{IV} + 3y^{IV}$ und die Rechnung, vermöge deren die Coefficienten von x^{IV} und y^{IV} sich bestimmen lassen, erhellt aus folgendem Schema (man vergl. hierüber den vorigen §.):

	1	—2	2	0
0	—1	2	5	—2
1	1	—3	—7	3

2) Indem wir im Verlaufe unserer Betrachtung auf den Begriff der reducirten Form geführt sind, so entsteht die Frage nach der Anzahl der reducirten Formen, die überhaupt möglich sind (wir betrachten hierbei natürlich nur solche reducirte Formen, die einerlei Determinante haben) und in welchem Verhältniss die verschiedenen möglichen reducirten Formen zu einander stehen. Nehmen wir den zweiten Punkt zuerst auf und suchen die Bedingungen dafür, dass zwei reducirte Formen mit einerlei Determinante einander aequivalent seien. Wir wollen bei dieser Untersuchung in voller Allgemeinheit sowohl den positiven, wie den negativen Zustand der äusseren Coefficienten einer Form zulassen.

Seien die betrachteten beiden reducirten Formen (a, b, c) und (a', b', c'), die gemeinschaftliche Determinante $-D$ und nehmen wir, wie es statthaft ist, $a' \overline{\overline{<}} a$ an. Wenn nun die beiden Formen einander (im eigentlichen Sinne) aequivalent sein sollen, so muss die erste Form in die zweite übergeben durch die Substitutionen $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ und es gelten die 3 Gleichungen:

$$(1) \quad \alpha\delta - \beta\gamma = 1$$

$$(2) \quad a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a' \qquad (3) \quad a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'.$$

Aus (2) folgt $(a\alpha + b\gamma)^2 + D\gamma^2 = aa'$, mithin ist aa' als Summe zweier positiven Grössen selbst positiv, d. h. a und a' müssen von gleichen Zeichen sein. Da nun a und c, a' und c' in Bezug auf das Vorzeichen gleichfalls übereinstimmen, so haben die 4 Grössen a, a', c, c' alle das nämliche Vorzeichen. Betrachten wir jetzt den Ausdruck $D\gamma^2 = aa' -$

$(a\alpha + b\gamma)^2$, so ist klar, da a und a' dasselbe Zeichen haben und absolut genommen nicht mehr als $\sqrt{\frac{1}{3}D}$ betragen dürfen, dass das Product aa' positiv und nicht mehr als $\frac{1}{3}D$ ist. Dem zu Folge ist noch stärker die positive Grösse $D\gamma^2$ nicht mehr als $\frac{1}{3}D$ und dieser Bedingung kann für ganzzahlige γ nur genügt werden, wenn man entweder $\gamma = 0$ oder $\gamma = \pm 1$ annimmt.

a) Nehmen wir $\gamma = 0$ an, so folgt aus (1) $\alpha\delta = 1$, also entweder $\alpha = 1$, $\delta = 1$ oder $\alpha = -1$, $\delta = -1$. In beiden Fällen zieht man aus (2) die Gleichheit $a = a'$ und aus (3) die andere Gleichheit $b' - b = \pm a\beta$, wo $b \leqq \frac{1}{2}a$, $b' \leqq \frac{1}{2}a' = \frac{1}{2}a$ sein muss, (natürlich gelten diese Ungleichungen nur für die absoluten Werthe und dasselbe wird selbstverständlich für die nachfolgenden Ungleichungen vorausgesetzt).

Haben nun b und b' gleiches Zeichen, so kann die Differenz $b' - b$ nur für $b' = b$ ein Vielfaches von a werden, nämlich dasjenige, welchem der Werth $\beta = 0$ entspricht. Daraus folgt aber die Identität der beiden Formen (a, b, c) und (a', b', c') im Widerspruche zu der Voraussetzung, nach der sie verschieden sind.

Also müssen wir b und b' als einander entgegengesetzt annehmen; dies vorausgesetzt kann aber die Differenz $b' - b$ nur für die Werthe $b' = \mp\frac{1}{2}a$, $b = \pm\frac{1}{2}a$ ein Vielfaches von a werden. Die Form (a', b', c') geht dann über in $(a, -b, c)$ und ist mithin zu der ersten Form (a, b, c) die entgegengesetzte mit der Nebenbedingung $2b = \pm a$.

b) Wenn $\gamma = \pm 1$ ist, so folgt aus (2) $a\alpha^2 + c - a' = \pm 2b\alpha$. Nun ist $c \geqq a$ zu Folge der Natur der reducirten Formen, $a \geqq a'$ nach der Voraussetzung, daher $c \geqq a'$ oder $c - a' \geqq 0$. Dies in Verbindung gebracht mit der letzten Gleichung zeigt, dass (absolut genommen) $2b\alpha \geqq a\alpha^2$ und dies dividirt durch die Ungleichung $2b \leqq a$ giebt $\alpha \geqq \alpha^2$, welches nur möglich ist entweder für $\alpha = 0$ oder für $\alpha = \pm 1$.

α) Sei $\alpha = 0$, so folgt aus (2) $c = a'$ und da $c \geqq a$, $a \geqq a'$, d. h. a zwischen c und a' enthalten ist, so ist nothwendig $c = a' = a$. Ferner ist wegen (1) $\beta\gamma = -1$ und dies, sowie ± 1 für γ in (3) einsetzend erhalten wir $b + b' = \pm c\delta$ oder $b + b' = \pm a\delta$ und die Werthe von b und b' hierin müssen wieder den Ungleichungen $b \leqq \frac{1}{2}a$, $b' \leqq \frac{1}{2}a$ genügen.

Haben b und b' beide gleiches Zeichen, so kann die Summe $b+b'$ nur unter der Annahme $b = b' = \pm\frac{1}{2}a$ ein Vielfaches von a geben; mithin wären gegen die Voraussetzung die beiden Formen (a, b, c) und (a', b', c') identisch.

Also müssen b und b' entgegengesetztes Zeichen haben und damit dann die Summe $b+b'$ ein Vielfaches von a werde, müssen auch ihre absoluten Werthe gleich sein, also $b = -b'$. Da in diesem Falle wegen Gleichheit der Determinanten noch $c = c'$ wird, so bekommt die Form (a', b', c') die Gestalt $a, -b, c)$ und wird mithin die entgegengesetzte zu der gegebenen Form (a, b, c): aber es muss noch die Nebenbedingung der Gleichheit der beiden äusseren Coefficienten eintreten, nämlich $a = c$.

β) Sei $\alpha = \pm 1$; dann folgt aus (2) $a+c-a' = \pm 2b$ und es ist mithin, da $a \geqq a'$ und $c \geqq a'$, $2b \geqq a$ und $2b \geqq c$. Andererseits ist aber auch zu Folge der Natur der reducirten Formen $2b \leqq a$, $2b \leqq c$ und damit diese verschiedenen Ungleichheiten für $2b$ einander nicht widersprechen, müssen sie übergehen in die Gleichheit $2b = a = c$. Da in der Gleichung $a+c-a' = 2b$ die Zahlen a, c, a' dasselbe Zeichen haben, so folgt jetzt weiter auch $a' = 2b$, also $2b = a = c = a'$. Endlich geht die Gleichung (3) wegen $c = a$ und $\alpha\delta = 1+\beta\gamma$ über in $a(\alpha\beta+\gamma\delta)+2(1+2\beta\gamma) = b'$ oder $a(\alpha\beta+\gamma\delta)+2b\beta\gamma = b'-b$ oder, wenn man für $2b$ den Werth $\pm a$ einsetzt, $b'-b = a(\alpha\beta+\gamma\delta\pm\beta\gamma)$.

Haben nun b und b' gleiches Zeichen, so kann die Differenz $b'-b$ nur so ein Vielfaches von a darstellen, dass man $b' = b$ hat, d. h. die beiden gegebenen Formen wären gegen die Voraussetzung identisch.

Also müssen b und b' ungleiches Vorzeichen haben und alsdann kann die Differenz $b'-b$ nur dadurch ein Multiplum von a werden, dass man setzt $b = \pm\frac{1}{2}a$, $b' = \mp\frac{1}{2}a$; die Form $(a' b', c')$ geht dann über in die Form $(a, -b, c)$ und ist der gegebenen Form (a, b, c) entgegengesetzt, mit den beiden Nebenbedingungen, dass man $2b = \pm a$ und die beiden äusseren Coefficienten a und c einander gleich hat.

Fassen wir das Ganze unserer Entwickelung zusammen, so bekommen wir das Theorem: Zwei reducirte Formen (a, b, c) und (a', b', c') sind einander aequivalent, erstens wenn sie einander entgegengesetzt sind mit der Nebenbedingung $2b =$

$\pm a$, und zweitens, wenn sie einander entgegengesetzt sind mit der Nebenbedingung der Gleichheit der beiden äusseren Coefficienten a und c.

Die Aequivalenz, von der hier die Rede ist, ist im eigentlichen Sinne gemeint. Indem also gewisse entgegengesetzte Formen als eigentlich aequivalent ausgesprochen werden, könnte dies als im Widerspruch zu einem früheren Theoreme stehend erscheinen, nach welchem alle entgegengesetzten Formen uneigentlich aequivalent sind. Der Widerspruch löst sich einfach auf durch die Bemerkung, dass im vorliegenden Falle die Aequivalenz eben so sehr im eigentlichen, wie im uneigentlichen Sinne statt hat.

Die beiden Formen (a, b, c) und $(a, -b, c)$ sind zunächst unter allen Umständen nach unserem allgemeinen Theoreme im vorigen Paragraphen einander im uneigentlichen Sinne aequivalent. Ist nun erstens die Nebenbedingung $a = c$ erfüllt, so kann man sie zu gleicher Zeit als angrenzende Formen ansehen und mithin als im eigentlichen Sinne einander aequivalent betrachten. Ist dagegen zweitens die Nebenbedingung $2b = \pm a$ erfüllt, so ist die Form (a, b, c) im eigentlichen Sinne aequivalent der Form $(c, -b, a)$ und diese letztere in Bezug auf ihre dritte Partie ist die angrenzende an die Form $(a, -b, c)$*). Da nun angrenzende Formen einander im eigentlichen Sinne aequivalent sind, so haben wir die Form $(c, -b, a)$ in demselben Sinne aequivalent sowohl der Form (a, b, c), wie auch der Form $(a, -b, c)$: mithin darf man die beiden letzteren als eigentlich aequivalent ansehen (cf. theor. 1 des vorigen §.).

Eine solche Form, wie die eben besprochene $(2b, b, c)$ oder allgemeiner eine Form (a, b, c) von der Beschaffenheit, dass der mittlere doppelte Coefficient $2b$ ein Multiplum des ersten Coeffienten a ist, hat Gauss eine zweideutige Form genannt; die Benennung rechtfertigt sich durch den Satz, dass eine

*) Die beiden Determinanten sind einander gleich; ferner ist der dritte Coefficient der ersten Form gleich dem ersten Coefficienten der zweiten Form und endlich ist $\frac{-b+(-b)}{a}$ ein ganzzahliger Ausdruck, weil $a = \pm 2b$ ist. — Uebrigens sind die an diese Untersuchung sich anknüpfenden und sogleich folgenden Erklärungen von der Natur der Determinante unabhängig.

solche Form sich selber ebensowohl im eigentlichen Sinne, wie im uneigentlichen Sinne aequivalent ist.

Die eigentliche Aequivalenz erhellt daraus, dass sie vermöge der Substitution $x = x' + 0 . y'$, $y = 0 . x' + y'$, welche der Bedingung $\alpha\delta - \beta\gamma = 1$ genügt, unverändert bleibt. Die uneigentliche Aequivalenz ergiebt sich auf folgende Weise. Die beiden Formen (c, b, a) und (a, b, c) sind, wenn $2b$ ein Multiplum von a ist, angrenzende Formen und daher eigentlich aequivalent; nun sind dieselben aber auch vermöge des Theoremes 8) im vorigen §. einander uneigentlich aequivalent. Indem also die Form (a, b, c) einmal der Form (c, b, a) eigentlich aequivalent und dann wieder der nämlichen Form uneigentlich aequivalent ist, muss sie vermöge des Theoremes 1) in dem eben erwähnten §. nothwendig sich selber uneigentlich aequivalent sein. In der That wird sie durch die Substitutionen $x = x' + \frac{2b}{a} y'$, $y = 0 . x' - y'$ nicht verändert und dieselben genügen der Bedingung $\alpha\delta - \beta\gamma = -1$, welche eine uneigentliche Transformation anzeigt.

Betrachten wir jetzt irgend zwei beliebige im eigentlichen Sinne aequivalente Formen F und F', so müssen die ihnen entsprechenden reducirten Formen f und f' gleichfalls aequivalent sein; die Formen f und f' sind alsdann entweder identisch oder entgegengesetzt, entweder mit der Bedingung, dass sie die beiden äusseren Coefficienten gleich haben, oder dass sie zweideutige sind. Umgekehrt, wenn die reducirten Formen f und f' entweder identisch sind oder zweideutig und einander entgegengesetzt oder entgegengesetzt mit Gleichheit der äusseren Coefficienten, so sind die ursprünglichen Formen F und F' im eigentlichen Sinne einander aequivalent.

Nehmen wir, um etwas Genaueres festzustellen, irgend zwei beliebige Formen F und F' an und bezeichnen die beiden entsprechenden reducirten Formen respective durch f und f', so sind überhaupt folgende verschiedene Fälle möglich: 1) f und f' sind weder identisch noch entgegengesetzt: dann sind F und F' weder eigentlich noch uneigentlich aequivalent; 2) f und f' sind entweder identisch und zugleich zweideutig, oder entgegengesetzt mit Gleichheit der beiden äusseren Coefficienten:

dann sind F und F' ebensowohl eigentlich wie uneigentlich einander aequivalent; 3) f und f' sind identisch und weder zweideutig noch haben sie die beiden äusseren Coefficienten gleich: dann sind F und F' nur im eigentlichen Sinne aequivalent; 4) f und f' sind entgegengesetzt, aber weder zweideutig, noch haben sie die äusseren Glieder gleich: dann sind F und F' nur im uneigentlichen Sinne einander aequivalent. — Der Beweis ergiebt sich durchweg einfach und stützt sich vornehmlich auf das Theorem 1) im vorigen Paragraphen.

3) Die nächstliegende Frage ist die, wie die verschiedenen auf eine gegebene Determinante $-D$ bezüglichen reducirten Formen (a, b, c) gefunden werden. Es ist hierbei genügend, alle diejenigen Formen aufzusuchen, in denen die beiden äusseren Coefficienten positiv sind; denn diejenigen mit negativen äusseren Coefficienten folgen aus den ersteren mit der grössten Leichtigkeit. Man kann nun auf einem doppelten Wege zum Ziele gelangen.

Erstens kann man für a der Reihe nach alle (positiven) Zahlen setzen, welche kleiner als $\sqrt{\frac{4}{3}D}$ sind und zu gleicher Zeit, da der Congruenz $b^2 \equiv -D \pmod{a}$ Genüge geschehen muss, zum quadratischen Reste die Zahl $-D$ haben. Die einzelnen Werthe von b werden dann erhalten, indem man die eben genannte Congruenz in den kleinsten Zahlen für b auflöst. Die Werthe von c bestimmen sich hierauf durch die Gleichung $c = \frac{b^2+D}{a}$. Wenn hierbei irgend welche Formen entstehen, in denen $a > c$ ausfällt, so sind dieselben zu verwerfen.

Zweitens kann man auch für b alle positiven oder negativen Zahlen annehmen, die nicht mehr als $\frac{1}{2}\sqrt{\frac{4}{3}D} = \sqrt{\frac{D}{3}}$ betragen und zerlege sich dann für die verschiedenen Werthe von b den Ausdruck b^2+D auf alle nur möglichen Weisen in je zwei (positive) Factoren, die jedoch beide nicht unter $2b$ sein dürfen. Hierauf setze man den einen Factor und zwar im Falle der Ungleichheit den kleineren gleich a, den anderen gleich c und verwerfe bei diesem Geschäfte noch alle die Combinationen, in denen a sich grösser als $\sqrt{\frac{4}{3}D}$ ausweist. Die auf diese Weise resultirenden Formen sind die sämmtlichen möglichen reducirten Formen.

Beispiel. Es sei $D = 85$. Alsdann liegt $\sqrt{\frac{4}{3}D}$ zwischen 10 und 11 und diejenigen positiven Zahlen, welche unter 11 sind und -85

zum quadratischen Reste haben, sind: 1, 2, 5, 10. Wir haben daher die 4 Congruenzen

$$b^2 \equiv -85 \ (mod\ 1), \ b^2 \equiv -85 \ (mod\ 2), \ b^2 \equiv -85 \ (mod\ 5),$$
$$b^2 \equiv -85 \ (mod\ 10)$$

aufzulösen; die Lösungen in den kleinsten Zahlen sind

$$b = 0, \ b = +1, \ -1, \ b = 0, \ b = +5, \ -5$$

und diesen Werthen von b entsprechend findet man der Reihe nach

$$c = 85, \ c = 43, \ c = 17, \ c = 11.$$

Hiernach ergeben sich folgende 6 reducirte Formen mit positiven äusseren Coefficienten:

(1, 0, 85), (2, 1, 43), (2, —1, 43), (5, 0, 17), (10, 5, 11), (10, —5, 11)

und eben so viele mit negativen äusseren Coefficienten:

(—1, 0, —85), (—2, —1, —43), (—2, 1, —43), (—5, 0, —17),
(—10, —5, —11), (—10, 5, —11).

Wendet man die andere Methode an, so sind die Grenzen, zwischen denen $\sqrt{\frac{D}{3}}$ liegt, die Zahlen 5 und 6. Die verschiedenen möglichen Annahmen für b sind daher $b = 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5$. Die Annahme $b = 0$ giebt $b^2 + D = 85$ und die Factorenzerlegungen hiervon sind 1.85 und 5.17, die ihnen entsprechenden Formen (1, 0, 85) und (5, 0, 17). Die Annahme $b = \pm 1$ giebt $b^2 + D = 86$ und man hat 86 = 1.86, 2.43. Die erste Factorenzerlegung ist unbrauchbar, weil der Factor 1 unterhalb $2b = 2$ liegt; die zweite liefert die beiden Formen: (2, 1, 43) und (2, —1, 43). Setzt man $b = \pm 2$, so wird $b^2 + D = 89$ und dies giebt überhaupt keine Zerlegung in 2 solche Factoren, die beide nicht unterhalb $2b = 4$ liegen; ebensowenig sind die Annahmen $b = \pm 3$ und $b = \pm 4$ statthaft. Endlich für $b = \pm 5$ wird $b^2 + D = 110$ und man hat die Zerfällungen 1.110, 2.55, 5.22, 10.11, von denen indessen nur die letzte brauchbar ist und die beiden Formen (10, 5, 11) und (10, —5, 11) liefert. Wir haben also schliesslich dieselben 6 Formen mit positiven äusseren Coefficienten gefunden, wie vorher.

Unter den 12 auf die Determinante —85 bezüglichen reducirten Formen sind jedoch mehrere Paare von (im eigentlichen Sinne) aequivalenten Formen; es sind dies die Paare von entgegengesetzten und zweideutigen Formen (2, 1, 43) und (2, —1, 43), sowie (10, 5, 11) und

(10, —5, 11), ausserdem noch die entsprechenden mit negativen äusseren Coefficienten. Indem wir von jedem dieser Paare nur die erste Form beibehalten und die letzte wegwerfen, bekommen wir folgende 8 auf die Determinante —85 bezüglichen und wesentlich von einander verschiedenen Formen:

(1, 0, 85), (2, 1, 43), (5, 0, 17), (10, 5, 11).
(—1, 0, —85), (—2, 1, —43), (—5, 0, —17), (—10, 5, —11).

Allgemein, wenn man sich die sämmtlichen auf eine bestimmte Determinante —*D* bezüglichen reducirten Formeln gebildet hat, so suche man unter denselben sich alle diejenigen aus, die einander im eigentlichen Sinne aequivalent sind, und werfe von jeder dadurch entstehenden Gruppe aequivalenter Formen alle bis auf eine weg. Die übrig bleibenden reducirten Formen haben die bemerkenswerthe Eigenthümlichkeit, dass jede beliebige Form, welche die nämliche Determinante —*D* besitzt, irgend einer und nur einer unter denselben (denn wären mehrere von dieser Art darunter, so wäre die eben erwähnte Ausscheidung nicht vollständig erfolgt) im eigentlichen Sinne aequivalent ist. Demgemäss zerfallen alle die unendlich vielen Formen, welche dieselbe Determinante —*D* haben, in eben so viele wesentlich von einander verschiedene Klassen, als nach der obigen Ausscheidung reducirte Formen übrig geblieben sind. Alle Formen einer und derselben Klasse sind einander eigentlich aequivalent, dagegen zwei Formen, welche verschiedenen Klassen angehören, können nicht eigentlich aequivalent sein. Nachfolgend möge folgende aus den „Disquisitiones arithmeticae“ des grossen Gauss entnommene Tabelle reducirter Formen einen Platz finden, die nach den oben auseinander gesetzten Principien entworfen ist, und der grösseren Kürze halber nur solche Formen enthält, deren äussere Coefficienten positiv sind:

Determ.	
—1	(1, 0, 1)
—2	(1, 0, 2)
—3	(1, 0, 3), (2, 1, 2)
—4	(1, 0, 4), (2, 0, 2)
—5	(1, 0, 5), (2, 1, 3)
—6	(1, 0, 6), (2, 0, 3)

Determ.	
—7	(1, 0, 7), (2, 1, 4)
—8	(1, 0, 8), (2, 0, 4), (3, 1, 3)
—9	(1, 0, 9), (2, 1, 5), (3, 0, 3)
—10	(1, 0, 10), (2, 0, 5)
—11	(1, 0, 11), (2, 1, 6), (3, 1, 4), (3, —1, 4)
—12	(1, 0, 12), (2, 0, 6), (3, 0, 4), (4, 2, 4).

Wir wollen, obwohl es überflüssig scheinen könnte, dennoch bemerken, dass unter den auf die beschriebene Art zurückbleibenden reducirten Formeln zwar keine sein können, die im eigentlichen Sinne aequivalent sind, wohl aber solche, die es im uneigentlichen Sinne sind; so z. B. für die Determinante —11 finden wir in der Tabelle die beiden Formen (3, 1, 4) und (3, —1, 4) verzeichnet, die als entgegengesetzt nothwendig uneigentlich aequivalente sind und zwar nur uneigentlich aequivalente, da in ihnen weder die beiden äusseren Coefficienten gleich sind, noch auch der erste Coefficient das Doppelte des zweiten ist.

4) Wenn zwei (eigentlich) aequivalente Formen $F = (A, B, A')$ und $f = (a, b, a')$ gegeben sind, eine Transformation der ersten Form in die zweite zu finden.

Man bestimme sich zunächst die beiden reducirten Formen zu F und f: dies geschehe durch die beiden Reihen angrenzender Formen:

$(A, B, A'), (A', B', A''), (A'', B'', A'''), \ldots (A^{(n-1)}, B^{(n-1)}, A^{(n)}), (A^{(n)}, B^{(n)}, A^{(n+1)})$
und
$(a, b, a'), (a', b', a''), (a'', b'', a'''), \ldots (a^{(m-1)}, b^{(m-1)}, a^{(m)}), (a^{(m)}, b^{(m)}, b^{(m+1)})$.

Alsdann sind folgende beide verschiedene Fälle möglich, die wir gleichmässig zu betrachten haben:

a) Die beiden reducirten Formen $(A^{(n)}, B^{(n)}, A^{(n+1)})$ und $(a^{(m)}, b^{(m)}, a^{(m+1)})$ sind entweder identisch oder entgegengesetzt und zu gleicher Zeit zweideutig; es ist also $A^{(n)} = a^{(m)}$, $B^{(n)} = \pm b^{(m)}$, $A^{(n+1)} = a^{(m+1)}$. Bemerken wir, dass zu Folge der Natur der angrenzenden Formen die beiden Congruenzen $B^{(n-1)} + B^{(n)} \equiv 0 \pmod{A^{(n)}}$ und $b^{(m-1)} + b^{(m)} \equiv 0 \pmod{a^{(m)}}$ bestehen, deren Modul einander gleich sind, so erhalten wir, indem wir $B^{(n-1)} + B^{(n)} \equiv b^{(m-1)} + b^{(m)}$ folgern und darauf $B^{(n)} \equiv b^{(m)}$ abziehen, die neue Congruenz $B^{(n-1)} - b^{(m-1)} \equiv 0 \pmod{a^{(m)}}$. Also sind die beiden Formen $(A^{(n-1)}, B^{(n-1)}, a^{(m)})$ und $(a^{(m)}, -b^{(m-1)}, a^{(m-1)})$ angrenzend an einander.

und wir können daher die beiden obigen Formenreihen unter Weglassung der beiden letzten zu Folge der Voraussetzung einander aequivalenten Formen, und nachdem wir die zweite, wie folgt, umgeschrieben haben:

$(a^{(m)}, -b^{(m-1)}, a^{(m-1)}), (a^{(m-1)}, -b^{(m-2)}, a^{(m-2)}), \ldots\ldots (a'', -b', a'),$
$(a' -b, a),$

zu einer einzigen zusammenschmelzen, nämlich

$(A, B, A'), (A', B', A''), \ldots\ldots (A^{(n-1)}, B^{(n-1)}, a^{(m)}), a((^{(m)}, -b^{(m-1)}, a^{(m-1)}),$
$a^{(m-1)}, -b^{(m-2)}, a^{(m-2)}), \ldots\ldots (a'', -b', a'), (a', -b, a), (a, b, a').$

Aus diesem letzteren kann aber nach dem im vorigen Paragraphen gelehrten Verfahren die Transformation der ersten Form in die letzte gefunden werden.

b) Die beiden reducirten Formen sind entgegengesetzt und haben gleiche äussere Coefficienten, d. h. es ist $A^{(n)} = A^{(n+1)} = a^{(m)} = a^{(m+1)}$, $B^{(n)} = -b^{(m)}$. Alsdann wendet man genau das eben angegebene Verfahren an, mit dem einzigen Unterschiede, dass man die letzte Form in der ersten Reihe beibehält, und bekommt durch Combination der beiden Reihen die zusammengesetzte:

$(A, B, A'), (A', B', A''), \ldots\ldots (A^{(n)}, B^{(n)}, a^{(m)}), (a^{(m)}, -b^{(m-1)}, a^{(m-1)}),$
$(a^{(m-1)}, b^{(m-2)}, a^{(m-2)}), \ldots\ldots (a'', -b', a'), (a', -b, a), (a, b, a').$

(Dass die beiden Formen $(A^{(n)}, B^{(n)}, a^{(m)})$ und $(a^{(m)}, -b^{(m-1)}, a^{(m-1)})$ angrenzende sind, erhellt daraus, dass man $B^{(n)} - b^{(m-1)} = -(b^{(m)} + b^{(m-1)})$ also durch $a^{(m)}$ ohne Rest theilbar hat). Vermöge dieser Formenreihe findet man wieder in bekannter Weise eine (eigentliche) Transformation der ersten Form in die letzte.

Auf der Auflösung dieser Aufgabe beruht nun unmittelbar die Lösung des wichtigen Problems: Zu finden, ob eine Form $F = (a, b, c)$ von gegebener Zusammensetzung eine gegebene Zahl M darzustellen fähig ist oder mit anderen Worten: die Gleichung $ax^2 + 2bxy + cy^2 = M$ in ganzen Zahlen für x und y aufzulösen.

Zunächst, damit das Problem eine Lösung zulasse, ist erforderlich, wenn auch noch nicht hinreichend, dass die Determinante $-D$ der gegebenen Form ein quadratischer Rest von M (nach §. 22, 1) sei. Dies vorausgesetzt löse man sich die alsdann immer mögliche Bedingungsgleichung $z^2 + D = Ms$ in den kleinsten Zahlen nach z und s auf und bilde, indem $z = \zeta$ und $s = \sigma$ irgend eine Lösung repräsentirt, die Form

(M, ζ, σ), so dass wir so viele derartige Formen erhalten, als verschiedene Lösungen der genannten Gleichung existiren. Hierauf vergleiche man jede derselben mit der gegebenen Form. Wenn sich nun herausstellt, dass keine darunter der gegebenen im eigentlichen Sinne aequivalent ist, so ist überhaupt keine Darstellung der Zahl M durch die Form (a, b, c) möglich, die zu irgend einer Lösung der Bedingungsgleichung gehören könnte; die gegebene Gleichung ist mithin unmöglich. Wenn dagegen eine oder mehrere darunter der gegebenen Form aequivalent sind, so bilde man die Transformationsformeln von F in jede solche Form (M, ζ, σ). Seien dieselben dargestellt, wie folgt: $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, so wird die Form (a, b, c) die Zahl M repräsentiren für das System der Werthe $x = \alpha$, $y = \gamma$ und dies Werthsystem stellt eine Lösung der Gleichung $ax^2 + 2bxy + cy^2 = M$ dar.

Beispiel. Die vorgelegte Gleichung sei

$$49x^2 - 118xy + 317y^2 = 2221, \quad -D = -12052.$$

Die Hülfsgleichung ist

$$z^2 + 12052 = 2221s.$$

Setzt man, um sie zu vereinfachen, $s = u + 5$, so geht sie über in $z^2 + 947 = 2221u$ oder $z^2 \equiv -947 \pmod{2221}$. Nachdem man durch Versuche die Gleichung $2221 . 4 = 19^2 + 9 . 947$ gefunden hat, ergiebt sich in bekannter Weise $\zeta = \pm 734$ und der entsprechende Werth von s wird $\sigma = 248$. Betrachten wir nun zuerst die Lösung $\zeta = -734$, $\sigma = 248$, welche auf die Form $(M, \zeta, \sigma) = (2221, -734, 248)$ führt, und suchen die reducirte Form zu letzterer, so bekommt man die reducirte Form als die letzte in der folgenden Reihe von Formen:

$$(2221, -734, 248), (248, -10, 49), (49, 10, 248).$$

Suchen wir ferner zu der gegebenen Form die reducirte, so erhalten wir die zweite Formenreihe:

$$(49, -59, 317), (317, 59, 49), (49, -10, 248).$$

Die beiden reducirten Formen sind also $(49, 10, 248)$ und $(49, -10, 248)$, d. h. entgegengesetzt, ohne im eigentlichen Sinne aequivalent zu sein. Also existirt keine Repräsentation von 2221 durch die gegebene Form, welche zu der Lösung $\zeta = -734$, $\sigma = 248$ der Hülfsgleichung gehören könnte.

Untersuchen wir jetzt die andere Lösung $\zeta = 734$, $\sigma = 248$, so sind die beiden zu vergleichenden Formen (2221, 734, 248) und (49, —59, 317) und wir erhalten die Formenreihen:

(2221, 734, 248), (248, 10, 49), (49, —10, 248)
(49, —59, 317), (317, 59, 49), (49, —10, 248).

Die beiden reducirten Formen sind identisch und es existirt mithin wenigstens eine Repräsentation von 2221 durch die gegebene Form, welche zu der Lösung $\zeta = 734$, $\sigma = 248$ gehört. Um dieselbe zu erhalten, bilde man sich aus den letzten beiden Formenreihen die zusammengesetzte:

(49, —59, 317), (317, 59, 49), (49, —10, 248), (248, —734, 2221), (2221, 734, 248)

und suche daraus die Transformation der gegebenen Form (49, —59, 317) in die letzte (2221, 734, 248); man findet $h' = \frac{-59+59}{317} = 0$, $h'' = \frac{59-10}{49} = 1$, $h''' = \frac{-10-734}{248} = -3$, $h^{IV} = \frac{-734+734}{2221} = 0$ und indem wir die in dem Schema

	0	1	—3	0
0	—1	—1	+4	1
1	0	—1	+3	1

angedeutete Rechnung benutzen, bekommen wir die Transformationsformeln $x = 4x' + y'$, $y = 3x' + y'$. Mithin ist $x = 4$ und $y = 3$ eine Lösung der vorgegebenen Gleichung.

Wir haben bisher beinahe durchweg nur solche Darstellungen einer Zahl M durch eine Form (a, b, c) ins Auge gefasst, in welchen die Werthe der Unbestimmten relative Primzahlen zu einander waren. Nehmen wir jetzt allgemein auch solche Werthe von x und y als zulässig an, die zum grössten gemeinschaftlichen Factor die Zahl μ haben, so ist die Form eines Lösungssystemes $x = \mu e$, $y = \mu f$, wo e und f relative Primzahlen zu einander bezeichnen. Substituiren wir diese Werthe in unsere Form, so erhalten wir $\mu^2(Ae^2 + 2Bef + Cf^2) = M$ und es erhellt daraus, dass M, damit die untersuchte Repräsentation ohne Widerspruch bestehen könne, nothwendig den Factor μ^2 besitzen müsse. **Mithin wenn eine Zahl M durch eine quadratische Form, sei es mit nega-**

tiver oder mit positiver Determinante, durch solche Werthe der Unbestimmten, die relative Primzahlen zu einander sind, darstellbar sein soll, so muss sie nothwendig wenigstens einen quadratischen Factor enthalten. In einem solchen Falle bestimme man sich alle möglichen quadratischen Theiler μ'^2, μ''^2, μ'''^2, ... von M und suche in bekannter Weise, indem μ^2 irgend einen dieser Theiler bezeichnet, diejenigen relativen Primzahlen von e und f, vermöge derer die Form (a, b, c) die Zahl $\frac{M}{\mu^2}$ repräsentirt; alsdann sind μe und μf diejenigen Werthe der Unbestimmten x und y, für welche dieselbe Form die Zahl M repräsentirt. Also führt die Aufsuchung aller solcher Lösungen der Gleichung $ax^2+2bxy+cy^2=M$, in welchen x und y nicht relative Primzahlen zu einander sind, auf den einfachen Fall zurück, in welchem sie solche sind.

Die Lösung des allgemeinen Problemes, welches uns beschäftigt, die Gleichung $ax^2+2bxy+cy^2=M$ in relativen Primzahlen für x und y aufzulösen, ist, was die Frage der Möglichkeit oder Unmöglichkeit betrifft und für den Fall einer negativen Determinante, mit aller nur wünschenswerthen Vollständigkeit durchgeführt; dagegen tritt es als ein Mangel hervor, dass wir, die Möglichkeit vorausgesetzt, vermöge der beschriebenen Methode eben nur eine einzige specielle Lösung erhalten; die Frage bleibt unerledigt, ob noch andere Lösungen existiren und, wenn dies der Fall sein sollte, wie viele es sind und auf welche Weise wir sie erhalten. Da jede Transformation der Form (a, b, c) in die Form (M, σ, ζ) uns eine specielle Lösung der vorgegebenen Gleichung liefert, so hängt diese Frage aufs innigste mit der anderen zusammen, wie viele solcher Transformationen existiren und auf welche Weise man sie erhalten kann. Diese Untersuchung soll später wieder aufgenommen werden; fürs erste aber wollen wir die Frage der Möglichkeit oder Unmöglichkeit unserer vorgelegten Gleichung auch noch für den Fall einer positiven Determinante erledigen.

§. 24.

Von den quadratischen Formen mit positiver nicht-quadratischer Determinante.

1) Indem wir jetzt die quadratischen Formen mit positiver Determinante näher betrachten, soll der Ausdruck $D = b^2 - ac$ eine wesentlich positive Grösse bedeuten, die keine vollständige Quadratzahl ist. Dies vorausgesetzt nehmen wir die Betrachtung der Reihe von angrenzenden Formen wieder auf, mit welcher der §. 22 schliesst, und untersuchen insbesondere das Gleichungssystem (A), vermöge dessen die erste Form der Reihe nach und nach alle übrigen liefert. Bestimmen wir daselbst die Grössen b', b'', b''', ... vermöge der Gleichungen $b+b' = a'h'$, $b'+b'' = a''h''$, $b''+b''' = a'''h'''$, ... derartig, dass sie, indem a', a'', a''', ... ohne Rücksicht aufs Vorzeichen und blos nach ihren absoluten Zahlenwerthen genommen werden (ebenso wie $\sqrt{D}$) respective zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} - a'$, $\sqrt{D}$ und $\sqrt{D} - a''$, $\sqrt{D}$ und $\sqrt{D} - a'''$, ... zu liegen kommen, etwas, was, wie leicht ersichtlich ist, nur auf eine einzige Art geschehen kann*): so ist zunächst ersichtlich, dass die absoluten Werthe der Grössen a', a'', a''', a^{IV}, ... nicht beständig abnehmen können; denn alsdann existirte eine unendliche Reihe beständig abnehmender ganzer Zahlen, was ein Widersinn wäre. Also, wenn man die Reihe nur weit genug fortsetzt, so ist man sicher irgend einmal auf eine Zahl $a^{(n-1)}$ zu stossen, welche nicht kleiner als $a^{(n)}$ ist. Die dieser Zahl

---

*) Alle die obigen Gleichungen stehen unter der Form $b^{(m-1)} + b^{(m)} = a^{(m)}h^{(m)}$ und $b^{(m)}$ muss, wenn Δ die kleinste in $\sqrt{D}$ enthaltene ganze Zahl bezeichnet, zwischen Δ und $\Delta - a^{(m)}$ liegen. Ist nun $a^{(m)}$ positiv, also Δ die obere Grenze, so setze man, indem h eine Zahl $< a^{(m)}$ bezeichnet, $b^{(m)} = \Delta - h$; dann ist die Bestimmung von $b^{(m)}$ identisch mit der Bestimmung der Grösse h vermöge der Congruenz $b^{(m-1)} + \Delta - h \equiv 0 \pmod{a^{(m)}}$, welche, wie wir wissen, nur eine einzige positive Lösung für h zwischen den Grenzen 0 und $a^{(m)}$ hat. Diese Lösung fällt nämlich mit dem kleinsten positiven Reste zusammen, welcher bei der Division von $b^{(m-1)} + \Delta$ durch $a^{(m)}$ erhalten wird. Ganz ähnlich beweist man, dass, wenn $a^{(m)}$ eine wesentlich negative Zahl, also $\Delta - a^{(m)}$ die obere Grenze für $b^{(m)}$ wird, gleichfalls ein und nur ein Werth der Grösse $b^{(m)}$ zwischen den angegebenen Grenzen möglich ist.

entsprechende Form $(a^{(n)}, b^{(n)}, a^{(n+1)})$, welche die letzte der Reihe sein wird, soll nun näher betrachtet werden.

Zu Folge der Bedingung, welcher die Wahl der Grösse $b^{(n)}$ unterworfen ist, liegt sie zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-[a^{(n)}]$, wo die eckige Klammer für den Augenblick als die Marke dafür dienen soll, dass $a^{(n)}$ nicht als algebraische Grösse, sondern nur nach seinem absoluten Zahlenwerthe in Rechnung kommt; mithin ist $\sqrt{D}$ die obere und $\sqrt{D}-[a^{(n)}]$ die untere Grenze. Daraus folgt weiter, dass, wenn man $\sqrt{D}-b^{(n)}=p$ und $b^{(n)}-(\sqrt{D}-[a^{(n)}])=q$ setzt, p und q wesentlich positive Zahlen vorstellen; mithin ist sowohl der Ausdruck $q^2+2pq+2p\sqrt{D}$ positiv, wie auch der damit gleichbedeutende $D+a^{(n)2}-b^{(n)2}$ oder auch, wenn man für D seinen Werth $b^{(n)2}-a^{(n)}a^{(n+1)}$ einsetzt, $a^{(n)2}-a^{(n)}a^{(n+1)}$. Da der absolute Werth von $a^{(n)}$ nicht mehr als der absolute Werth von $a^{(n+1)}$ sein darf, so ist dies nicht anders möglich, als wenn $a^{(n)}$ und $a^{(n+1)}$ verschiedene Zeichen haben. Dies vorausgesetzt ergiebt sich aus der Gleichung $b^{(n)2}=D+a^{(n)}a^{(n+1)}$, dass $b^{(n)2}<D$, also $[b^{(n)}]<\sqrt{D}$; der mittlere Coefficient $b^{(n)}$ ist also seinem absoluten Werthe nach kleiner als die (gleichfalls im absoluten Sinne genommene) $\sqrt{D}$.

Ferner die Gleichung $-a^{(n)}a^{(n+1)}=D-b^{(n)2}$, wo die linke Seite nach der oben gemachten Bemerkung wesentlich positiv ist, hat zu Folge die Ungleichung $[a^{(n)}][a^{(n+1)}]<D$ und mithin muss, da wir gemäss der Voraussetzung $[a^{(n)}]\leqq[a^{(n+1)}]$ haben, $[a^{(n)}]<\sqrt{D}$ sein, d. h. die Differenz $\sqrt{D}-[a^{(n)}]$ ist eine wesentlich positive Grösse. Demgemäss sind die beiden Grenzen, zwischen denen $b^{(n)}$ enthalten ist, beide positiv, und also auch $b^{(n)}$ selbst; um so stärker hat man $\sqrt{D}-[a^{(n)}]+b^{(n)}$ als einen positiven Ausdruck. Nun ist aber der Ausdruck $\sqrt{D}-[a^{(n)}]-b^{(n)}$, weil er gleich $-q$ ist, wesentlich negativ: also liegt $[a^{(n)}]$ zwischen den Grenzen $\sqrt{D}+b^{(n)}$ und $\sqrt{D}-b^{(n)}$; denn die Ungleichungen $\sqrt{D}-[a^{(n)}]+b^{(n)}>0$ und $\sqrt{D}-[a^{(n)}]-b^{(n)}<0$, welchen man auch die Gestalt $\sqrt{D}+b^{(n)}>[a^{(n)}]$ und $\sqrt{D}-b^{(n)}<[a^{(n)}]$ geben kann, kann man zusammenschreiben, wie folgt:

$$\sqrt{D}+b^{(n)}>[a^{(n)}]>\sqrt{D}-b^{(n)}.$$

Eine Form (A, B, C), wie die oben betrachtete, deren Determinante gleich der positiven Zahl D, in welcher der mittlere Coefficient positiv und kleiner als $\sqrt{D}$ und der

erste Coefficient A seinem absoluten Werthe nach zwischen $\sqrt{D}+B$ und $\sqrt{D}-B$ liegt, heisst eine (auf die positive Determinante D bezügliche) reducirte Form. Die reducirten Formen mit positiver Determinante haben daher eine andere Natur, als die reducirten Formen mit negativer Determinante; indessen ist die gleiche Benennung von Gauss, dem Schöpfer dieser ganzen Theorie, eingeführt worden wegen der grossen Analogie, die demungeachtet zwischen beiderlei Arten von reducirten Formen herrscht.

Es erhellt jetzt unmittelbar, wenn man $A = a^{(n)}$, $B = b^{(n)}$, $C = a^{(n+1)}$ setzt, wie man von jeder beliebig gegebenen Form (a, b, a') vermöge einer Reihe von angrenzenden Formen zu der zugehörigen reducirten Form (A, B, C) gelangen kann.

Beispiel. Es sei die gegebene Form $(a, b, a') = (67, 97, 140)$, also $D = 29$, $\sqrt{D}$ zwischen 5 und 6, so findet man (cf. §. 22 das Formelsystem A) am Schlusse) die reducirte Form $(A, B, C) = (-1, 5, 4)$ auf folgende Art:

$(a, b, a') = (67, 97, 140)$; $5 \geqq b' > 5 - 140$, $-97 + b' = 140h'$, $b' \equiv 43 \pmod{140}$, $b' = -97$, $h' = 0$, $a'' = 67 - 0(97+97) = 67$;

$(a', b', a'') = (140, -97, 67)$; $5 \geqq b'' > 5 - 67$, $-97 + b'' = 67h''$, $b'' \equiv 30 \pmod{67}$, $b'' = -37$, $h'' = -2$, $a''' = 140 + 2(-97+37) = 20$;

$(a'', b'', a''') = (67, -37, 20)$; $5 \geqq b''' > 5 - 20$, $-37 + b''' = 20h'''$, $b''' \equiv 17 \pmod{20}$, $b''' = -3$, $h''' = -2$, $a^{IV} = 67 + 2(-37+3) = -1$;

$(a''', b''', a^{IV}) = (20, -3, -1)$; $5 \geqq b^{IV} > 5 - 1$, $-3 + b^{IV} = -h^{IV}$, $b^{IV} \equiv 1 \pmod{1}$, $b^{IV} = 5$ $h^{IV} = -2$, $a^{V} = 20 + 2(-3-5) = 4$;

$(a^{IV}, b^{IV}, a^{V}) = (-1, 5, 4)$.

Setzt man die Rechnung weiter fort, so erhält man noch die folgenden, wie sich ausweist, gleichfalls reducirten Formeln:

$(4, 3, -5)$, $(-5, 2, 5)$, $(5, 3, -4)$, $(-4, 5, 1)$, $(1, 5, -4)$,
$(-4, 3, 5)$, $(5, 2, -5)$, $(-5, 3, 4)$, $(4, 5, -1)$, $(-1, 5, 4)$

und, wenn man noch weiter geht, so wird man finden, dass die eben genannte Reihe reducirter Formeln unendlich oft wiederkehrt.

Wir stellen noch folgende Reihen auf, in welchen die jedesmalige letzte Form die reducirte zu der ersten Form ist:

$(20, -14, 4)$, $(4, 14, 20)$, $(20, 6, -4)$, $(-4, 10, 4)$;
$(956, 366, 140)$, $(140, -86, 52)$, $(52, -18, 4)$, $(4, 10, -4)$.

Die vorliegende Rechnung liefert den Beweis, dass mindestens 10 reducirte Formen, nämlich (—1, 5, 4), (4, 3, —5), (—5, 2, 5), ... zu der gegebenen Form (67, 97, 140) existiren, die sowohl unter einander, als auch der gegebenen aequivalent sein müssen. Zugleich zeigt ihre Betrachtung, dass, unter der Voraussetzung einer positiven Determinante, die Bedingungen, unter welchen reducirte Formen aequivalent sind, durchaus nicht die nämlichen und auch nicht so einfach sind, wie in dem Falle einer negativen Determinante. Ehe wir daher in unserer Untersuchung weiter gehen, wird es gut sein, wenn wir nach dem Vorgange von Gauss eine vorläufige genauere Kenntniss der Eigenheiten uns zu erwerben suchen, welche die reducirten Formen der betrachteten Art auszeichnen.

a) Wenn die Form (a, b, c) eine reducirte ist, so haben die beiden äusseren Coefficienten a und c entgegengesetzte Vorzeichen. Dies erhellt unmittelbar aus der Gleichung $ac = b^2 - D$, wenn man bedenkt, dass $b > \sqrt{D}$ ist.

b) Wenn die Form (a, b, c) eine reducirte ist, so ist jeder der beiden äusseren Coefficienten a und c zwischen den Grenzen $\sqrt{D}+b$ und $\sqrt{D}-b$ gelegen; es ist mithin auch die umgekehrte Form (c, b, a) eine reducirte. Dass a zwischen den erwähnten Grenzen liegt, folgt aus der Erklärung der reducirten Formen; dass das Nämliche auch von c gilt, ergiebt sich, wenn man bemerkt, dass wegen der Gleichung $c = \frac{D-b^2}{a}$ offenbar c zwischen den Grenzen $\frac{D-b^2}{\sqrt{D}+b}$ und $\frac{D-b^2}{\sqrt{D}-b}$, d. i. zwischen den Grenzen $\sqrt{D}-b$ und $\sqrt{D}+b$ liegt.

c) Jeder der beiden äusseren Coefficienten ist (absolut genommen) kleiner als $2\sqrt{D}$; der mittlere Coefficient b liegt zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-a$ (indem a in diesem Ausdrucke nicht als algebraische Zahl, sondern als absoluter Zahlenwerth gilt). Das Erste folgt aus den beiden Ungleichungen a oder $c < \sqrt{D}+b$ und $b < \sqrt{D}$; das Zweite folgt aus den Ungleichungen $a-(\sqrt{D}-b)$ oder $b-(\sqrt{D}-a) > 0$ und $b-\sqrt{D} > 0$. Ebenso lässt sich zeigen, dass b auch noch zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-c$ enthalten ist.

c) **Jeder reducirten Form ist in Bezug auf jeden ihrer beiden äusseren Coefficienten eine und nur eine reducirte Form angrenzend.**

Sei die gegebene reducirte Form (a, b, a') und in der angrenzenden Form (a', b', a'') die Grösse b' als die zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-[a']$ (wo die Hakenklammer, wie früher festgesetzt und weiter festgehalten werden soll, bedeutet, dass a' nicht als algebraische Zahl, sondern nur nach seinem absoluten Zahlenwerthe betrachtet werden soll) enthaltene Lösung der unbestimmten Gleichung $b+b'=a'h'$ bestimmt: so existirt immer eine und nur eine Form dieser Art. Wir haben nun zunächst zu beweisen, dass diese Form eine reducirte ist.

Zu Folge der Voraussetzung ist die untere Grenze für b' die Quantität $\sqrt{D}-[a']$ und die obere Grenze für $[a']$ die Quantität $\sqrt{D}+b$; daraus ergeben sich die beiden Ungleichungen $b'-\sqrt{D}+[a']>0$ und $b+\sqrt{D}-[a']>0$, welche zusammenaddirt die dritte Ungleichung $b+b'>0$ hervorbringen, d. h. $b+b'$ ist eine positive Grösse. Da nun $b+b'=a'h'$ ist, so folgt, dass h' dasselbe Zeichen hat, wie a' und eine von 0 verschiedene Grösse ist; mithin ist auf jeden Fall $[h']-1$ keine negative Grösse, also entweder positiv oder gleich 0.

Indem wir nun die vorige Gleichung also umschreiben: $b+b'=[a'][h']$ und darauf die Ungleichung $b'-\sqrt{D}+[a']>0$ hinzuaddiren, erhalten wir $2b'+b-\sqrt{D}+[a']>[a'].[h']$, oder um so stärker, wenn wir links für b die jedenfalls noch grössere Quantität $\sqrt{D}$ substituiren und einige leichte Umformungen vornehmen, $2b'>[a'].([h']-1)$. Nun ist die rechte Seite dieser Ungleichung keinesfalls negativ, mithin kann auch die linke Seite nicht negativ sein, d. h. wir haben im Allgemeinen b' als eine positive Grösse (die in speciellen Fällen jedoch sich annulliren kann). Da b' ferner seiner Bestimmung gemäss kleiner als $\sqrt{D}$ ist, so genügt der mittlere Coefficient den Bedingungen einer reducirten Form.

Aus der Gleichung $b+b'=[a'][h']$ ergiebt sich ferner, wenn man für b seine obere Grenze $\sqrt{D}$ einsetzt, $\sqrt{D}+b'>[a'][h']$, woher $\sqrt{D}+b'-[a']>[a']([h']-1)$; daher ist die linke Seite der vorstehenden Ungleichung positiv, also $\sqrt{D}+b'>[a']$. Es ist ferner, weil $\sqrt{D}-[a']$ die untere Grenze für b' ist, $\sqrt{D}-b'<[a']$, also bestehen die beiden Un-

gleichungen $\sqrt{D}-b' < [a'] < \sqrt{D}+b'$. Die untersuchte Form ist daher eine reducirte.

Dass keine zweite davon verschiedene und gleichfalls an (a, b, a') angrenzende Form, wie z. B. (a', β', α'') existiren könne, beweist man, wie folgt. Weil (a', β', α'') eine reducirte Form sein soll, ist β' nach dem Satze *c*) zwischen $\sqrt{D}$ und $\sqrt{D}-[a']$ enthalten und zu gleicher Zeit eine Wurzel der Congruenz $b+\beta \equiv 0$ $(mod\ [a'])$. Zwischen den nämlichen Grenzen liegt nun auch das vermöge der Congruenz $b+b' \equiv 0$ $(mod\ [a'])$ bestimmte b'. Da diese beiden Congruenzen identisch sind und innerhalb des in Frage kommenden Intervalles nur eine einzige Lösung besitzen, so muss man $b' = \beta'$ haben, d. h. die Form (a', b', a'') ist mit der Form $(a'\ \beta'\ \alpha'')$ identisch.

Also existirt nur eine einzige reducirte Form (a', b', a''), welche der gegebenen Form (a, b, a') in Bezug auf deren letzte Partie angrenzend ist. Ganz ebenso beweist man, dass nur eine einzige reducirte Form (a_1, b_1, a) existirt, welche der gegebenen Form (a, b, a') in Bezug auf deren erste Partie angrenzend ist.

e) Die Anzahl der reducirten Formen, die sich auf eine positive Determinante beziehen, ist begrenzt; die verschiedenen möglichen Formen können vermöge einer doppelten Methode erhalten werden.

Erstens man nimmt für a der Reihe nach alle Zahlen an, welche positiv und kleiner als $2\sqrt{D}$ sind und, damit der Congruenz $b^2 \equiv D$ $(mod\ a)$ Genüge geschehe, zum quadratischen Reste die Zahl D haben; hierauf setze man für b diejenigen den verschiedenen Werthen von a entsprechenden und in den kleinsten positiven Zahlen ausgedrückten Lösungen der eben genannten Congruenz, welche zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-a$ enthalten sind; die Grösse a' endlich ergiebt sich, indem man die Werthe des Ausdruckes $\frac{b^2-D}{a}$ für die verschiedenen zusammengehörigen Werthe von a und b berechnet. Alle hierbei etwa hervorgehenden Formen, in denen a ausserhalb der Grenzen $\sqrt{D}+b$ und $\sqrt{D}-b$ liegt, sind wegzuwerfen. Die übrigbleibenden Formen stellen alle nur möglichen von der Gestalt $(a, b, -a')$ dar, wo a und a' positive Grössen bezeichnen. Man findet eben so viele davon verschiedene, in denen der erste Coefficient

eine negative Grösse ist, indem man in den vorhergehenden entweder die Vorzeichen der beiden äusseren Coefficienten vertauscht oder indem man sie umkehrt, d. h. nach einer von Gauss eingeführten Benennung sich die associirten Formeln bildet. Unter einer associirten Form zu einer gegebenen nämlich versteht man diejenige Form, welche aus der gegebenen durch Vertauschung der beiden äusseren Coefficienten entsteht.

Zweitens kann man für b der Reihe nach alle nur irgend möglichen positiven ganzen Zahlen unterhalb der Grenze $\sqrt{D}$ annehmen und hierauf zusehen, ob die diesen verschiedenen Werthen von b entsprechenden Werthe des Ausdruckes die Zerfällung in zwei solche Factoren gestatten, deren absolute Werthe sich zwischen den Grenzen $\sqrt{D}+b$ und $\sqrt{D}-b$ befinden und von denen der erste eine positive Grösse darstellt. Jede derartige Factorenverbindung $a.-a'$ giebt alsdann die beiden associirten Formen $(a, b, -a')$ und $(-a', b, a)$.

Wir wollen beispielsweise vermöge der zweiten Methode die reducirten Formen der Determinante $D=79$ berechnen, für welche $\sqrt{D}$ zwischen den Grenzen 8 und 9 liegt. Die verschiedenen Werthe von b, die man der Reihe nach zu untersuchen hat, sind 1, 2, 3, 4, 5, 6, 7, 8. Setzen wir $b=1, 2$, so wird $b^2-D=-78, -75$ und es sind überhaupt keine Zerfällungen möglich, so dass die Factoren zwischen den Grenzen $\sqrt{D}+b$ und $\sqrt{D}-b$, d. h. hier zwischen den Grenzen 9, 11 und 9, 7 (dieselben incl.) zu liegen kommen. Setzen wir $b=3$, so wird $b^2-D=-70$ und die Grenzen für die Factoren der einzelnen zulässigen Zerfällungen werden $\sqrt{D}+b=8+3$ und $\sqrt{D}-b=9-3$, d. h. 11 und 6. Wir erhalten als die zwei allein statthaften Zerfällungen $+7.-10$ und $+10.-7$, wodurch die 4 Formen hervorgehen: $(7, 3, -10)$ und $(-10, 3, 7)$, $(10, 3, -7)$ und $(-7, 3, 10)$. Dieselben können auch wie folgt zusammengeschrieben werden: $(\pm 7, 3, \mp 10)$ und $(\pm 10, 3, \mp 7)$. Indem man in ähnlicher Weise fortgeht, ergeben sich nach und nach alle nur möglichen reducirten Formen mit der Determinante 79, nämlich:

$(\pm 7, 3, \mp 10)$, $(\pm 10, 3 \mp 7)$; $(\pm 7, 4, \mp 9)$, $(\pm 9, 4, \mp 7)$;
$(\pm 6, 5, \mp 9)$, $(\pm 9, 5, \mp 6)$; $(\pm 2, 7, \mp 15)$, $(\pm 15, 7, \mp 2)$;
$(\pm 3, 7, \mp 10)$, $(\pm 10, 7, \mp 3)$; $(\pm 2, 7, \mp 15)$, $(\pm 15, 7, \mp 2)$;
$(\pm 1, 8, \mp 15)$, $(\pm 15, 8, \mp 1)$; $(\pm 3, 8, \mp 5)$, $(\pm 5, 8, \mp 3)$.

Beispiel 2. Die auf die Determinante 133 bezüglichen reducirten Formeln sind:

$(\pm 11, 1, \mp 12)$, $(\pm 12, 1, \mp 11)$; $(\pm 9, 4, \mp 13)$, $(\pm 13, 4, \mp 9)$;
$(\pm 9, 5, \mp 12)$, $(\pm 12, 5, \mp 9)$; $(\pm 6, 7, \mp 14)$, $(\pm 14, 7, \mp 6)$;
$(\pm 7, 7, \mp 12)$, $(\pm 12, 7, \mp 7)$; $(\pm 4, 9, \mp 13)$, $(\pm 13, 9, \mp 4)$;
$(\pm 3, 10, \mp 11)$, $(\pm 11, 10, \mp 3)$; $(\pm 1, 11, \mp 12)$, $(\pm 12, 11, \mp 1)$;
$(\pm 2, 11, \mp 6)$, $(\pm 6, 11, \mp 2)$; $(\pm 3, 11, \mp 4)$, $(\pm 4, 11, \mp 3)$.

2) **Sämmtliche auf eine bestimmte Determinante D bezügliche Formen gruppiren sich in Perioden, deren jede eine gerade Anzahl lauter unter einander verschiedener und (eigentlich) aequivalenter Formen umfasst. Die Formen einer solchen Periode lassen sich derartig ordnen, dass immer je eine der nachfolgenden und die letzte der ersten angrenzend ist.**

Sei, um dieses zu beweisen, $F = (a, b, -a_1)$, wo a und a_1 Grössen von gleichem Vorzeichen bezeichnen, irgend eine reducirte Form und werde, wie gewöhnlich, $D = b^2 - aa_1$ gesetzt. Bilden wir uns die Reihe der angrenzenden Formen $F_1 = (-a_1, b_1, a_2)$, $F_2 = (a_2, b_2, -a_3)$, ... und zwar vermittelst des in der vorigen Nummer auseinandergesetzten Bildungsgesetzes, so erhellt aus d), dass jede Form dieser Reihe eine reducirte und in unzweideutiger Weise bestimmt ist, und es muss im Verlaufe der Rechnung die Form F auf jeden Fall noch einmal wieder hervortreten, so dass $F^{(n)}$ die erste Form der Reihe ist, welche der Anfangsform F gleich wird. Nämlich, da die Anzahl der reducirten Formen eine beschränkte ist, so kann die Reihe, die ersichtlich ins Unendliche fortgeht, nicht lauter von einander verschiedene Formen enthalten, also wenigstens eine specielle Form $F_m = (\pm a_m, b_m, \mp a_{m+1})$ der Reihe wird nothwendig irgend einmal zum zweiten Male auftreten, so dass man $F_m = F_{m+n}$ hat. Dies vorausgesetzt folgt $F_{m-1} = F_{m+n-1}$; denn die Formen $(\mp a_{m-1}, b_{m-1}, \pm a_m)$ und $(\mp a_{m+n-1}, b_{m+n-1}, \pm a_{m+n})$ sind nothwendig identisch, da man wegen Identität der Formen F_m und F_{m+n} die Gleichungen $\pm a_m = \pm a_{m+n}$, $b_m = b_{m+n}$ hat und demgemäss die dritten Coefficienten der betrachteten Formen die nämlichen sind und die mittelsten vermöge identischer Rechnungen gefunden werden. Indem man in derselben Weise weiter fortgeht, erhalten wir $F_{m-2} = F_{m+n-2}$, $F_{m-3} =$

$F_{m+n-3}, \ldots. F_1 = F_{n+1}, F = F_n$. Wir haben jetzt noch darzuthun, dass die Formen $F, F_1, F_2, F_3, \ldots. F_{n-1}$ alle unter einander verschieden sind, d. h. dass F_n die erste Form der Reihe ist, welche gleich F wird.

Zu Folge der Voraussetzung ist zwischen F_m und F_{m+n} keine Form enthalten, die identisch mit F_m oder, was dasselbe sagt, mit F_{m+n} wäre. Wenn nun innerhalb des Intervalles F_m und F_{m+n} zwei von F_m verschiedene und untereinander identische Formen $F\mu$ und $F\nu$ existirten, so dass ν und μ Zahlen innerhalb der Grenzen m und $m+n$ und $\nu > \mu$ wäre, so würde geschlossen werden dürfen $F\mu-1 = F\nu-1$, $F\mu-2 = F\nu-2, \ldots\ldots$ $F_m = F(\nu-\mu+m)$; nun sind ν und μ beides Zahlen kleiner als $n+m$, aber grösser als m; mithin $\nu-\mu+m$ eine zwischen m und $n+m$ befindliche Zahl, d. h. es existirt gegen die Voraussetzung innerhalb des Intervalles von F_m bis zu F_{m+n} eine dritte Form $F(\nu-\mu+n)$ identisch mit den beiden Formen F_m und F_{m+n}.

Also sind alle Formen zwischen F_m und F_{m+n} verschieden, folglich sind es auch die mit diesen der Reihe nach identischen Formen zwischen F und F_n, und die Reihe angrenzender Formen, welche mit F beginnt, wird sich aus derselben unendlich oft wiederkehrenden Periode zusammensetzen, welche die untereinander verschiedenen reducirten Formen $F, F_1, F_2, F_3, F_4, \ldots. F_{n-2}, F_{n-1}$ enthält.

Jede Form dieser Periode ist zu der nachfolgenden die angrenzende (zu Folge der Entstehung der Reihe); die letzte Form dagegen hat zu ihrer angrenzenden Form die erste. In der That sind F_{n-1} und F_n angrenzende Formen; da nun F und F_n identisch sind, so ist die Form F in Bezug auf ihre erste Partie die angrenzende zu der ersten Form.

Es bleibt noch zu beweisen, dass die Periode eine gerade Anzahl von Gliedern umfasst. Zu Folge der eingeführten Bezeichnung sind a, $a_1, a_2, a_3, \ldots\ldots a_{n-1}, a_n$ lauter Grössen von gleichem Vorzeichen; wenn wir mithin unter F_m eine beliebige Form verstehen, so wird der erste Coefficient dasselbe Vorzeichen mit a oder ein verschiedenes Vorzeichen haben, je nachdem der Index m eine gerade oder ungerade Zahl ist. Nun ist F identisch mit F_n, also a und a_n Grössen von gleichem Vorzeichen, also ist n gerade und mithin auch die Anzahl der in unserer Periode enthaltenen Formen.

Dieses Alles vorausgesetzt bilde man sich sämmtliche auf die Determinante D bezüglichen reducirten Formen und suche die auf die erste derselben bezügliche Periode. Dadurch werden eine Anzahl von Formen ausgeschieden, die wir als die Formen der ersten Periode bezeichnen können. Von den übrig bleibenden nehme man wieder die erste und bilde dazu in bekannter Weise die Reihe der angrenzenden Formen: dieselbe giebt die Formen der zweiten Periode und man wird sich dessen versichert halten können, dass keine Form der ersten Periode identisch ist mit irgend einer Form der zweiten Periode. Dies folgt aus einem Satze, den wir später beweisen werden, dass zwei aequivalente reducirte Formen nur Formen einer und derselben Periode und nicht Formen von einander verschiedener Perioden sein können. In ähnlicher Weise geht man weiter fort und bildet aus den übrig gebliebenen Formen die dritte, vierte, fünfte Periode und so weiter, bis keine mehr übrig ist. Die Formen irgend einer bestimmten Periode sind alle einander (im eigentlichen Sinne) aequivalent und es werden in den übrigen Perioden keine mit ihnen aequivalente Formen angetroffen.

Beispiel 1. Die zurückgeführten Formen der Determinante 79 zerfallen in folgende 6 Perioden:

I. (1, 8, —15), (—15, 7, 2), (2, 7, —15), (—15, 8, 1).

II. (—1, 8, 15), (15, 7 —2), (—2, 7, 15), (15, 8, —1).

III. (3, 8, —5), (—5, 7, 6), (6, 5, —9), (—9, 4, 7), (7, 3, —10), (—10, 7, 3).

IV. (—3, 8, 5), (5, 7, —6), (—6, 5, 9), (9, 4, —7), (—7, 3, 10), (10, 7, —3).

V. (5, 8, —3), (—3, 7, 10), (10, 3, —7), (—7, 4, 9), (9, 5, —6), (—6, 7, 5).

VI. (—5, 8, 3), (3, 7, —10), (—10, 3, 7), (7, 4, —9), (—9, 5, 6), (6, 7, —5).

Beispiel 2. Die zurückgeführten Formen der Determinante 133 geben folgende 4 Klassen:

I. (11, 1, —12), (—12, 11, 1), (1, 11, —12), (—12, 1, 11), (11, 10, —3), (—3, 11, 4), (4, 9, —13), (—13, 4, 9), (9, 5, —12), (—12, 7, 7), (7, 7, —12), (—12, 5, 9), (9, 4, —13), (—13, 9, 4), (4, 11, —3), (—3, 10, 11).

II. (—11, 1, 12), (12, 11, —1), (—1, 11, 12), (12, 1, —11),
(—11, 10, 3), (3, 11, —4), (—4, 9, 13), (13, 4, —9),
(—9, 5, 12), (12, 7, —7), (—7, 7, 12), (12, 5, —9),
(—9, 4, 13), (13, 9, —4), (—4, 11, 3), (3, 10, —11).

III. (6, 7, —14), (—14, 7, 6), (6, 11, —2), (—2, 11, 6).

IV. (—6, 7, 14), (14, 7, —6), (—6, 11, 2), (2, 11, —6).

Wir machen rücksichtlich dieser Perioden noch nachfolgende Bemerkungen:

a) Bildet man sich von zwei aequivalenten Formen die zugehörigen Perioden, so enthalten beide dieselben Formen und auch in derselben Ordnung und nur rücksichtlich des Anfanges und des Endes sind sie von einander verschieden; z. B. die Periode II. im ersten Beispiele kann auf doppelte Weise, wie folgt, beschrieben werden: (—1, 8, 15), (15, 7, —2), (—2, 7, 15), (15, 8, —1) oder (—2, 7, 15), (15, 8, —1), (—1, 8, 15), (15, 7, —2).

b) Wenn zwei zurückgeführte Formen associirt sind, so enthalten die zugehörigen Perioden lauter associirte Formen, und zwar sind solche Formen die beiden ersten, darauf die zweite, dritte, vierte, ... der einen mit respective der letzten, zweitletzten, drittletzten ...... Form der andern Periode. Zwei Perioden von der Beschaffenheit, dass die Formen der einen den Formen der anderen respective associirt sind, heissen associirte Perioden und auf dies Verhältniss kann schon aus der Existenz eines einzigen derartigen Paares associirter Formen geschlossen werden. Beispiele hierzu geben die auf die Determinante 79 bezüglichen Perioden III und VI, IV und V; dagegen von den auf die Determinante 183 bezüglichen Perioden sind keine je zwei einander associirt. — Wenn 2 Perioden associirt sind, so sind die Formen der einen den Formen der andern uneigentlich aequivalent. Der Beweis aller dieser Sätze ist leicht; der letzte namentlich beruht auf den Theoremen 1) und 3) in §. 22.

c) Wenn in einer Periode irgend eine Form und zugleich die ihr associirte vorkommt, so existirt zu jeder anderen Form in der nämlichen Periode die associirte. Eine solche Periode heisst sich selber associirt und es existiren darin jedes Mal zwei zweideutige Formen und nicht mehr.

Ordnen wir die Periode so, dass die eine der beiden associirten Formen den Anfang macht und sei dieselbe von der Gestalt F, F_1, F_2, F_3, ... F_{2n-2}, F_{2n-1}, so ist der Index der zu F associirten Form $< 2n$ und nothwendig eine ungerade Zahl, weil der erste Coefficient darin ein anderes Zeichen hat als der erste Coefficient in F. Setzen wir sie daher gleich F_{2m+1}. Man kann alsdann allmälig und ohne besondere Schwierigkeit den Nachweis führen, dass auch F_1 und F_{2m}, F_2 und F_{2m-1}, ... und allgemein F_k und F_{2m+1-k} associirte Formen sind. Da k und $2m+1-k$ niemals identisch werden können, so ist hiermit der erste Theil unseres Satzes bewiesen. Setzen wir nun $k=m$, so bekommen wir die angrenzenden Formen F_m und F_{m+1} als solche, die zugleich associirt sind und daher unter der allgemeinen Form $(A, B, -A')$ und $(-A', B, A)$ stehen; mithin folgt $B+B \equiv 0 \ (mod\ [A'])$ oder $2B$ durch A' ohne Rest theilbar. Daher ist F_{m+1} eine zweideutige Form. Setzen wir ferner $k = n+m$, so bekommen wir noch zwei andere angrenzende und zugleich associirte Formen, nämlich F_{n+m} und F_{n+m+1}; von denselben muss daher wieder die zweite eine zweideutige Form sein. Mehr zweideutige Formen aber als die eben aufgestellten können nicht existiren; denn zwischen den Grenzen F und F_{2n} kommen nicht mehr als zwei Paare aufeinanderfolgender Formen vor, die associirte sind, und wenn ausser jenen noch eine davon verschiedene dritte zweideutige Form existirt, so würde diese die Existenz eines dritten von den vorhergehenden verschiedenen Paares aufeinander folgender und associirter Formen zur Folge haben.

In der That, nehmen wir an, $F_{\lambda+1}$ sei eine zweideutige Form und λ von m und $m+n$ verschieden, so sind die beiden Formen F_λ und $F_{\lambda+1}$ aneinandergrenzend und mithin, wenn wir sie uns unter der Gestalt $(A, B, -A')$ und $(-A', B', A'')$ darstellen, hat man $B+B' \equiv 0 \ (mod\ [A'])$. Nun ist, weil $F_{\lambda+1}$ eine zweideutige Form ist, auch $B' \equiv 0 \ (mod\ [A'])$; also $B \equiv 0 \ (mod\ [A'])$. Da die Formen F_λ und $F_{\lambda+1}$ beide reducirte sind, so liegt nach dem Satze unter c) in der vorigen Nummer sowohl B, wie B' zwischen den nämlichen Grenzen D und $D-[A']$; da ferner die beiden Congruenzen, vermöge deren sie bestimmt werden, identisch sind und zwischen den genannten Grenzen nur eine Lösung gestatten, so folgt die Identität von B und B'. Die Gleichheit der Determinante endlich liefert $A = A''$. Also sind die beiden aufeinander folgenden Formen

F_λ und $F_{\lambda+1}$ associirt; d. h. es existirt zwischen den Grenzen F und F_{2n} noch ein drittes Paar associirter Formen, die unmittelbar aufeinander folgen.

Dass dies ein Widerspruch ist, ergiebt sich auf folgende Art. Da F_λ und $F_{\lambda+1}$ associirt sind, so sind es auch $F_{\lambda-1}$ und $F_{\lambda+2}$, $F_{\lambda-2}$ und $F_{\lambda+3}$, ... zuletzt F und $F_{2\lambda+1}$. Da nun aber F auch mit F_{2m+1} associirt ist, so müssen die Formeln $F_{2\lambda+1}$ und F_{2m+1} identisch sein, d. h. die Indices $2\lambda+1$ und $2m+1$ können nur um ein Vielfaches von $2n$ unterschieden sein, oder es wird der Congruenz $\lambda \equiv m \pmod n$ genügt. Dies wird für die Werthe $\lambda = m$, $m+n$ der Fall sein, welche indessen zu Folge der Annahme ausdrücklich ausgeschlossen sind; ausserdem geschieht es für die Werthe $\lambda = m+2n$, $m+3n$, $m+4n$, ...: aber schon der erste dieser Werthe ist unbrauchbar und noch stärker sind es die nachfolgenden. Denn, wenn wir $\lambda = m+2n$ setzen, so liegen die Formen F_λ und $F_{\lambda+1}$ ausserhalb der Grenzen F und F_{2n}, im Widerspruche mit der Annahme, nach der $F_{\lambda+1}$ die dritte zweideutige Form zwischen den genannten Grenzen sein soll. Diese Annahme hat daher überhaupt keinen Sinn.

Es lässt sich nun leicht auch der umgekehrte Satz nachweisen, dass jede Periode, in der eine zweideutige Form auftritt, sich selber associirt ist, und dass mithin die Existenz einer zweideutigen Form immer die Existenz von einer und nur einer zweiten in der nämlichen Periode zur Folge hat.

Dies folgt unmittelbar, da wir vorhin bewiesen haben, dass, wenn in irgend einer Periode eine Form, etwa $F_{\lambda+1}$, zweideutig ist, sie mit der vorhergehenden associirt sein muss, was, wie wir wissen, die Periode als mit sich selber associirt charakterisirt. Ebenso lässt sich ohne alle Schwierigkeit darthun, dass eine mit sich selber associirte Periode lauter Formen enthält, die sowohl im eigentlichen wie im uneigentlichen Sinne einander aequivalent sind.

Beispiele zu den vorstehenden Sätzen geben die sämmtlichen auf die Determinante 133 bezüglichen Perioden. So sind z. B. die beiden zweideutigen Formen in der Periode I: (1, 11, —12) und (7, 7, —12) und sonst sind weiter keine vorhanden.

d) Die Anwendung der Satzes unter d) in voriger Nummer legt es nahe, die Reihe der angrenzenden Formen F, F_1, F_2, F_3, ... auch nach links hin über F hinaus fortzusetzen; bedienen wir uns, um die dadurch sich ergebenden neuen Formen zu bezeichnen, der negativen Indices, so bekommen wir die nach beiden Seiten hin unbegrenzte Reihe:

$$\ldots\ldots F_{-2n}, F_{-2n+1}, \ldots\ldots F_{-2}, F_{-1}, F, F_1, F_2, \ldots\ldots F_{2n-1}, F_{2n}, \ldots\ldots$$

oder auch

$$\ldots\ldots (a_{-2}, b_{-2}, -a_{-1}), (-a_{-1}, b_{-1}, a), (a, b, -a_1), (-a_1, b_1, a_2) \ldots\ldots$$

und die Grössen a, ... a_{-2}, a_{-1}, a, a_1, a_2, ... sind hier sämmtlich mit dem gleichen Vorzeichen versehen.

Zugleich erhellt unmittelbar, dass man links von F dieselbe Periode erhält, wie rechts, und zwar sind F_{-1}, F_{-2}, F_{-3}, ... der Reihe nach identisch mit F_{2n-1}, F_{2n-2}, F_{2n-3}, ... Man hat daher das allgemeine Theorem, dass irgend zwei Formen der nach beiden Seiten hin unbegrenzten Reihe mit einander identisch oder von einander verschieden sind, je nachdem die respectiven Indices nach dem Modul $2n$ mit einander congruent oder incongruent sind. — Was die Quotienten ...... $\frac{b_{-3}+b_{-2}}{a_{-2}}$, $\frac{b_{-2}+b_{-1}}{-a_{-1}}$; $\frac{b_{-1}+b}{a}$, $\frac{b+b_1}{-a_1}$, $\frac{b_1+b_2}{a_2}$; ...... anbetrifft, die bei der Bildung der Reihe vorkommen und nachher, wie wir wissen, zur Transformation der ursprünglichen Form F in irgend eine beliebige der Reihe ihre Verwendung finden: so kann man dieselben, wie folgt, darstellen:

$$\ldots\ldots h_{-2}, -h_{-1}, h, -h_1, h_2, \ldots\ldots,$$

wo die sämmtlichen h, mögen sie nun positive oder negative Indices haben, dasselbe Vorzeichen haben wie a. Die absoluten Werthe der der Periode rechts von F entsprechenden h sind der Reihe nach h_1, h_2, h_3, ... h_{2n-1}, die absoluten Werthe der der Periode links von F entsprechenden h sind gleichfalls der Reihe nach h, h_{-1}, h_{-2}, h_{-3}, ... h_{2n-2} und man hat wieder allgemein den Satz, dass je zwei h mit ungleichen Indices identisch oder nicht identisch sind, je nachdem die Indices nach dem Modul $2n$ einander congruent sind oder incongruent.

3) Betrachten wir jetzt näher die Transformation einer reducirten Form F in irgend eine andere Form der zugehörigen Periode und unter-

suchen die Modificationen, welche die allgemeine in §. 22 unter 3) auseinandergesetzte Lösung dieses Problemes in dem gegenwärtigen Falle erfährt. Zu dem Zwecke schreiben wir uns wieder die Reihe der angrenzenden Formen sammt den dazu gehörigen Werthen der verschiedenen h hin, wie folgt:

$$\ldots\ldots F_{-4},\ F_{-3},\ F_{-2},\ F_{-1},\ F,\ F_1,\ F_2,\ F_3,\ F_4,\ldots\ldots$$
$$-h_{-3},\ h_{-2},\ -h_{-1},\ h,\ -h_1,\ h_2,\ -h_3,\ h_4$$

und fassen zunächst die Transformation der Form F in irgend eine Form F_m mit positivem Index ins Auge. Nehmen wir an, dass sie sich durch die Substitutionen $x = \alpha_m x_m + \beta_m y_m$, $y = \gamma_m x_m + \delta_m y_m$ vollziehe: alsdann wissen wir, dass man die Coefficienten α_m und β_m als die respective den Partialquotienten $\pm h_{m-1}$ und $\mp h_m$ entsprechenden Glieder einer Reihe erhält, welche in ähnlicher Weise sich bildet, wie die aufeinanderfolgenden Zähler der Näherungswerthe zu einem gegebenen Kettenbruche, und die Coefficienten γ_m und δ_m als die nämlichen Partialquotienten entsprechenden Glieder einer anderen Reihe, deren Bildung ähnlich ist wie die Bildung der aufeinanderfolgenden Nenner zu einem gegebenen Kettenbruche. Die Quotienten $\frac{\alpha_m}{\gamma_m}$ und $\frac{\beta_m}{\delta_m}$ müssen daher etwas Aehnliches darstellen, wie zwei solche aufeinanderfolgende Näherungsbrüche.

Indem wir daher die aufeinanderfolgenden Werthe der Grössen α_m und γ_m für die verschiedenen Werthe von m berechnen und ihre absoluten Zahlenwerthe respective durch A_m und C_m bezeichnen, erhalten wir nach und nach unter der Annahme, dass a und mithin auch h_1, h_2, ... positiv sind, folgende Resultate:

$$\begin{array}{ll}
\alpha_1 = \quad 0 = +A_1, & \gamma_1 = \quad 1 \; = +C_1 \\
\alpha_2 = -1 = -A_2, & \gamma_2 = -h_1 = -C_2 \\
\alpha_3 = -A_2 .\ \ h_2-(+A_1) = -(A_2h_2+A_1) = -A_3, & \gamma_3 = -(C_2h_2+C_1) = -C_3 \\
\alpha_4 = -A_3 .-h_3-(-A_2) = +(A_3h_3+A_2) = +A_4, & \gamma_4 = +(C_3h_3+C_2) = +C_4 \\
\alpha_5 = +A_4 .\ \ h_4-(-A_3) = +(A_4h_4+A_3) = +A_5, & \gamma_5 = +(C_4h_4+C_3) = +C_5 \\
\alpha_6 = +A_5 .-h_5-(+A_4) = -(A_5h_5+A_4) = -A_6, & \gamma_6 = -(C_5h_5+C_4) = -C_6 \\
\alpha_7 = -A_6 .\ \ h_6-(+A_5) = -(A_6h_6+A_5) = -A_7, & \gamma_7 = -(C_6h_6+C_5) = -C_7 \\
\ldots\ldots\ldots & \ldots\ldots\ldots \\
\ldots\ldots\ldots & \ldots\ldots\ldots
\end{array}$$

und daraus:

$\beta_1 = -A_2,\ \beta_2 = -A_3,\ \beta_3 = +A_4,\ \beta_4 = +A_5,\ \beta_5 = -A_6,\ \beta_6 = -A_7, \ldots.$
$\delta_1 = -C_2,\ \delta_2 = -C_3,\ \delta_3 = +C_4,\ \delta_4 = +C_5,\ \delta_5 = -C_6,\ \delta_6 = -C_7, \ldots.$

Wenn wir dagegen die Grösse a und mit ihr alle die verschiedenen h negativ haben, so folgen die vier Gleichungssysteme:

$\alpha_1 = -A_1,\ \alpha_2 = -A_2,\ \alpha_3 = +A_3,\ \alpha_4 = +A_4,\ \alpha_5 = -A_5,\ \alpha_6 = -A_6, \ldots.$
$\gamma_1 = +C_1,\ \gamma_2 = +C_2,\ \gamma_3 = -C_3,\ \gamma_4 = -C_4,\ \gamma_5 = +C_5,\ \gamma_6 = +C_6, \ldots.$
$\beta_1 = -A_2,\ \beta_2 = +A_3,\ \beta_3 = +A_4,\ \beta_4 = -A_5,\ \beta_5 = -A_6,\ \beta_6 = +A_7, \ldots.$
$\delta_1 = +C_2,\ \delta_2 = -C_3,\ \delta_3 = -C_4,\ \delta_4 = +C_5,\ \delta_5 = +C_6,\ \delta_6 = -C_7, \ldots.$

Aus dieser Analyse ergiebt sich, dass die absoluten Zahlenwerthe der Coefficienten in den Substitutionen, vermöge deren F in irgend welche Form seiner Periode übergeht, sowohl wenn a positiv ist, wie auch wenn a negativ ist, dieselben bleiben und dass die Vorzeichen in beiden Fällen nach einem leicht zu übersehenden Gesetze wechseln. Wir werden daher grösserer Einfachheit halber in dieser Nummer a vorzugsweise als positiv annehmen, so dass auch die Grössen h_1, h_2, h_3, ..., sowie die Grössen h_{-1}, h_{-2}, h_{-3}, ... als positiv angesehen werden müssen. In der That kommt es in den unmittelbar nachfolgenden Entwickelungen auch nur auf die absoluten Werthe der genannten Coefficienten, d. h. auf die Werthe der verschiedenen A und C an.

Dieses vorausgesetzt sieht man unmittelbar ein, dass die Grössen A_1, A_2, A_3, A_4, ... und C_1, C_2, C_3, ... genau die nämliche Bildung haben, wie respective die Zähler und Nenner der Näherungswerthe zu einem Kettenbruche, dessen Partialquotienten die ganzen positiven Zahlen h_1, h_2, h_3, h_4, ... sind, der also die Form zeigt:

$$\cfrac{1}{h_1 + \cfrac{1}{h_2 + \cfrac{1}{h_3 + \cfrac{1}{h_4 + \ldots..}}}}$$

Hiervon scheinen nur die beiden Werthe $\alpha_1 = 0$ und $\gamma_1 = 1$ ausgenommen. Indessen ordnen sich auch diese demselben Gesetze unter, wenn man als 0ten Näherungswerth die Grösse $\frac{0}{1}$ annimmt, wie wir ja schon von der Bildung der Näherungswerthe her es gewohnt sind. Es hindert nun nichts, dass wir den Index m über jede Grenze hinaus wachsen lassen, d. h. dass wir den Kettenbruch als einen unendlichen uns denken. Zu Folge der Erörterungen p. 45, 46, 47 wissen wir, dass der Werth

eines solchen Kettenbruches eine endliche Quantität ist und es entsteht die Frage, wie er gefunden werden kann. Da der Kettenbruch ein periodischer ist, d. h. in seinen Partialquotienten die beständige Wiederholung der Zahlen h_1, h_2, h_3, ... h_{2n} darbietet, so schliessen wir nach dem Theoreme, welches sich p. 53 am Schlusse befindet, dass er irgend eine der beiden Wurzeln einer quadratischen Gleichung darstellt. Um das Genauere hierüber festzustellen, gehen wir auf die Entstehung der Partialquotienten h_1, h_2, h_3, ... zurück, welche sich in folgenden Gleichungen ausspricht:

$$\sqrt{D} > b_1 > \sqrt{D} - a_1, \quad \frac{b+b_1}{a_1} = h_1, \quad D = b_1^2 + aa_1;$$

$$\sqrt{D} > b_2 > \sqrt{D} - a_2, \quad \frac{b_1+b_2}{a_2} = h_2, \quad D = b_1^2 + a_1 a_2;$$

$$\sqrt{D} > b_3 > \sqrt{D} - a_3, \quad \frac{b_2+b_3}{a_3} = h_3, \quad D = b_2^2 + a_2 a_3;$$

. . . .

. . . .

Betrachten wir jetzt den Werth von $\frac{b+b_1}{a_1}$, so haben wir wegen der beiden Grenzwerthe von b_1 die Ungleichung $\frac{\sqrt{D}+b}{a_1} > \frac{b+b_1}{a_1} > \frac{\sqrt{D}+b-a_1}{a_1}$ oder $\frac{\sqrt{D}+b}{a_1} > h_1 > \frac{\sqrt{D}+b}{a_1} - 1$ oder endlich, wenn man eine leichte Umformung vornimmt:

$$h_1 + 1 > \frac{\sqrt{D}+b}{a_1} > h_1.$$

Dies heisst in Worten nichts anderes, als der Werth des Ausdruckes $\frac{\sqrt{D}+b}{a_1}$ ist zwischen den ganzen Zahlen h_1 und h_1+1 enthalten oder auch h_1 ist die nächst kleinere ganze Zahl, welche in dem Ausdruck enthalten ist. Mithin darf man, indem u vorläufig eine positive Quantität kleiner als 1 bezeichnet, $\frac{\sqrt{D}+b}{a_1} = h_1 + u$ setzen, woher $\frac{a_1}{\sqrt{D}+b} = \frac{1}{h_1+u}$. Setzt man hier für die Grösse links den Ausdruck $\frac{a_1(\sqrt{D}-b)}{D-b^2} = \frac{\sqrt{D}-b}{a}$ und rechts für u seinen Werth $\frac{\sqrt{D}+b}{a_1} - h_1 = \frac{\sqrt{D}+b}{a_1} - \frac{b+b_1}{a_1} = \frac{\sqrt{D}-b_1}{a_1}$, so bekommen wir die Gleichung

$$\frac{\sqrt{D}-b}{a}=\frac{1}{h_1+\frac{\sqrt{D}-b_1}{a_1}}$$

Die Betrachtung der Grenzen, innerhalb derer die Ausdrücke $\frac{b_1+b_2}{a_2}$, $\frac{b_2+b_3}{a_3}$, $\frac{b_3+b_4}{a_4}$, ... liegen, liefert genau in der nämlichen Weise die Gleichungen:

$$\frac{\sqrt{D}-b_1}{a_1}=\frac{1}{h_2+\frac{\sqrt{D}-b_2}{a_2}},\quad \frac{\sqrt{D}-b_2}{a_2}=\frac{1}{h_3+\frac{\sqrt{D}-b_3}{a_3}},\ \ldots\ldots$$

und man sieht leicht ein, wie sich diese Gleichungen ins Unbegrenzte fortsetzen. Substituiren wir in jede Gleichung von der ersten ab die nachfolgende, so erhalten wir:

$$\frac{\sqrt{D}-b}{a}=\frac{1}{h_1+\frac{1}{h_2+\frac{1}{h_3+\ldots\ldots+\frac{1}{h_{2n-1}+\frac{1}{h_{2n}+\frac{1}{h_1+\ldots\ldots}}}}}}$$

Gehen wir weiter zur Transformation der Form F in irgend eine Form F_{-m} fort, und nehmen wir an, dass die umgekehrten Formen $(-a_1, b, a)$ und $(\mp a_{-m+1}, b_{-m}, \pm a_m)$ in einander übergehen durch die Substitutionen $x=\delta_{-m}x_{-m}+\gamma_{-m}y_{-m}$, $y=\beta_{-m}x_{-m}+\alpha_{-m}y_{-m}$: so werden die Zahlenwerthe von δ_{-m}, γ_{-m}, β_{-m}, α_{-m} vermöge der Zahlenwerthe h, $-h_{-1}$, h_{-2}, $-h_{-3}$, ... genau ebenso berechnet, wie vorhin die Zahlenwerthe von α_m, β_m, γ_m, δ_m vermöge der Zahlenwerthe von $-h_1$, h_2, $-h_3$, ..., und die gesuchte Transformation von F in F_{-m} wird erhalten, wenn man in den eben aufgestellten Formeln die Unbestimmten x und y, x_{-m} und y_{-m} mit einander vertauscht, d. h. sie vollzieht sich vermöge der Substitutionen:

$$x=\alpha_{-m}x_{-m}+\beta_{-m}y_{-m},\quad y=\gamma_{-m}x_{-m}+\delta_{-m}y_{-m}.$$

Die Coefficienten α_{-m} und β_{-m} in diesen Formeln lassen sich daher berechnen als den Partialquotienten h_{-m} und h_{-m+1} entsprechende Glieder einer Reihe, welche vermöge der Reihe h, $-h_{-1}$, h_{-2}, $-h_{-3}$, ... von Partialquotienten eine ähnliche Bildung hat, wie die Nenner der aufeinanderfolgenden Näherungswerthe eines Kettenbruches, und die Coefficienten

γ_{-m} und δ_{-m} als die denselben Partialquotienten entsprechenden Glieder einer Reihe, die vermöge der nämlichen Reihe von Partialquotienten in ähnlicher Weise entsteht, wie die Zähler der aufeinanderfolgenden Näherungswerthe zu einem Kettenbruche. Nach dieser Regel bekommen wir unter der Annahme eines positiven a, indem die verschiedenen Grössen B und D lauter absolute Zahlenwerthe bezeichnen, folgende Coefficientenbestimmung:

$$\begin{array}{ll}
\beta = 1 = +B, & \delta = 0 = -D \\
\beta_{-1} = k = +B_{-1} & \delta_{-1} = -1 = -D_{-1} \\
\beta_{-2} = -(B_{-1}k_{-1}+B) = -B_{-2}, & \delta_{-2} = +(D_{-1}k_{-1}+D) = +D_{-2} \\
\beta_{-3} = -(B_{-2}k_{-2}+B_{-1}) = -B_{-3}, & \delta_{-3} = +(D_{-2}k_{-2}+D_{-1}) = +D_{-3} \\
\beta_{-4} = +(B_{-3}k_{-3}+B_{-2}) = +B_{-4}, & \delta_{-4} = -(D_{-3}k_{-3}+D_{-2}) = -D_{-4} \\
\beta_{-5} = +(B_{-4}k_{-4}+B_{-3}) = +B_{-5}, & \delta_{-5} = -(D_{-4}k_{-4}+D_{-3}) = -D_{-5} \\
\beta_{-6} = -(B_{-5}k_{-5}+B_{-4}) = -B_{-6}, & \delta_{-6} = +(D_{-5}k_{-5}+D_{-4}) = +D_{-6} \\
\cdots\cdots\cdots & \cdots\cdots\cdots \\
\cdots\cdots\cdots & \cdots\cdots\cdots
\end{array}$$

und

$$\alpha = +B_{-1},\ \alpha_{-1} = -B_{-2},\ \alpha_{-2} = -B_{-3},\ \alpha_{-3} = +B_{-4},\ \alpha_{-4} = +B_{-5},\ \alpha_{-5} = -B_{-6},\ \ldots\ldots$$

$$\gamma = -D_{-1},\ \gamma_{-1} = +D_{-2},\ \gamma_{-2} = +D_{-3},\ \gamma_{-3} = -D_{-4},\ \gamma_{-4} = -D_{-5},\ \gamma_{-5} = +D_{-6},\ \ldots\ldots$$

Für ein negatives a dagegen erhält man:

$$\beta = +B,\ \beta_{-1} = -B_{-1},\ \beta_{-2} = -B_{-2},\ \beta_{-3} = +B_{-3},\ \beta_{-4} = +B_{-4},\ \beta_{-5} = -B_{-5},\ \ldots\ldots$$

$$\delta = +D,\ \delta_{-1} = -D_{-1},\ \delta_{-2} = -D_{-2},\ \delta_{-3} = +D_{-3},\ \delta_{-4} = +D_{-4},\ \delta_{-5} = -D_{-5},\ \ldots\ldots$$

$$\alpha = -B_{-1},\ \alpha_{-1} = -B_{-2},\ \alpha_{-2} = +B_{-3},\ \alpha_{-3} = +B_{-4},\ \alpha_{-4} = -B_{-5},\ \alpha_{-5} = -B_{-6},\ \ldots\ldots$$

$$\gamma = -D_{-1},\ \gamma_{-1} = -D_{-2},\ \gamma_{-2} = +D_{-3},\ \gamma_{-3} = +D_{-4},\ \gamma_{-4} = -D_{-5},\ \gamma_{-5} = -D_{-6},\ \ldots\ldots$$

Hieraus erhellt gerade wie vorher, dass die Bestimmung der Vorzeichen, welche die Coefficienten haben müssen, in leichter Weise für sich abgemacht werden kann und überhaupt das Vorzeichen von a auf die absoluten Werthe der Coefficienten keinen Einfluss übe. Indem wir daher die Grösse a der Einfachheit halber als wesentlich positiv annehmen, kön-

nen wir die Zahlengrössen B, B_{-1}, B_{-2}, ... und D, D_{-1}, D_{-2}, ... als identisch mit den aufeinanderfolgenden Zählern und Nennern betrachten, welche entstehen, wenn man sich die Näherungswerthe bildet zu dem Kettenbruche:

$$h+\frac{1}{h_{-1}+\frac{1}{h_{-2}+\frac{1}{h_{-3}+\ldots\ldots}}}$$

wo die Partialquotienten h, h_{-1}, h_{-2}, h_{-3}, ... lauter positive ganze Zahlen bezeichnen. Lassen wir den Index $-m$ über jede Grenze hinauswachsen, so wird dieser Kettenbruch unendlich und sein Werth wird gefunden durch Betrachtung der Grenzen, zwischen denen die Zahlenwerthe von $h=\frac{b_{-1}+b}{a}$, $h_{-1}=\frac{b_{-2}+b_{-1}}{a_{-1}}$, $h_{-2}=\frac{b_{-3}+b_{-2}}{a_{-2}}$, ... enthalten sind. Diese Betrachtung hat nach einander die Gleichungen zu Folge:

$$\frac{\sqrt{D}+b}{a}=h+\frac{1}{\frac{\sqrt{D}+b_{-1}}{a_{-1}}},\quad \frac{\sqrt{D}+b_{-1}}{a_{-1}}=h_{-1}+\frac{1}{\frac{\sqrt{D}+b_{-2}}{a_{-2}}},$$

$$\frac{\sqrt{D}+b_{-2}}{a_{-2}}=h_{-2}+\frac{1}{\frac{\sqrt{D}+b_{-3}}{a_{-3}}},\ \ldots\ldots,$$

die sich ins Unendliche fortsetzen lassen und aus denen durch Substitution einer jeden in die vorhergehende fliesst:

$$\frac{\sqrt{D}+b}{a}=h+\frac{1}{h_{-1}+\frac{1}{h_{-2}+\frac{1}{h_{-3}+\ldots+\frac{1}{h_{-2n+2}+\frac{1}{h_{-2n+1}+\frac{1}{h+\ldots}}}}}}$$

Vergleichen wir diesen letzten Kettenbruch, der die Transformation von F in F_{-m} giebt, mit dem ersten, der der Transformation von F in F_m entspricht, so ist $h=h_{2n}$, $h_{-1}=h_{2n-1}$, $h_{-2}=h_{2n-2}$, ... $h_{-2n+1}=h_1$, d. h. die Periode des einen ist die umgekehrte Periode des anderen. Gemäss dem Theoreme, welches p. 53 am Ende aufgestellt wurde, müssen daher die Werthe beider dem absoluten Werthe nach die Wurzeln einer und derselben quadratischen Gleichung darstellen. Diese Gleichung ist $ax^2-2bx=a_1$; die Wurzeln derselben sind $x=\frac{\sqrt{D}+b}{a}$ und $x=-\frac{\sqrt{D}-b}{a}$ und der genannte Satz mithin verificirt.

Um ein praktisches Beispiel zu haben, wollen wir die Periode der Form $F=(3,\ 8,\ -5)$ betrachten; wir bekommen dadurch folgendes Schema, in welchem sich rechts die Substitutionen befinden, vermöge derer die Form F in irgend eine gleichnamige übergeht und zwar der grösseren Kürze halber allein die Coefficienten der Unbestimmten. (So z. B. ist die Substitution, vermöge welcher F in F_{-7} übergeht, $x=-805x_{-7}-152y_{-7}$ und $y=143x_{-7}+27y_{-7}$):

		$\alpha_{-m},\ \alpha_m$	$\beta_{-m},\ \beta_m$	$\gamma_{-m},\ \gamma_m$	$\delta_{-m},\ \delta_m$
$F_{-7}=(-10,\ 7,\ 3)$		-805	-152	$+143$	$+27$
	$h_{-6}=+5$				
$F_{-6}=(3,\ 8,\ -5)$		-152	$+45$	$+27$	-8
	$h_{-5}=-3$				
$F_{-5}=(-5,\ 7,\ 6)$		$+45$	$+17$	-8	-3
	$h_{-4}=2$				
$F_{-4}=(6,\ 5,\ -9)$		$+17$	-11	-3	$+2$
	$h_{-3}=-1$				
$F_{-3}=(-9,\ 4,\ 7)$		-11	-6	$+2$	$+1$
	$h_{-2}=1$				
$F_{-2}=(7,\ 3,\ -10)$		-6	$+5$	$+1$	-1
	$h_{-1}=-1$				
$F_{-1}=(-10,\ 7,\ 3)$		$+5$	$+1$	-1	0
	$h=5$				
$F=(3,\ 8,\ -5)$		$+1$	0	0	$+1$
	$h_1=-3$				
$F_1=(-5,\ 7,\ 6)$		0	-1	1	-3
	$h_2=2$				
$F_2=(6,\ 5,\ -9)$		-1	-2	-3	-7
	$h_3=-1$				
$F_3=(-9,\ 4,\ 7)$		-2	$+3$	-7	$+10$
	$h_4=1$				
$F_4=(7,\ 3,\ -10)$		$+3$	$+5$	$+10$	$+17$
	$h_5=-1$				
$F_5=(-10,\ 7,\ 3)$		$+5$	-8	$+17$	-27
	$h_6=5$				
$F_6=(3,\ 8,\ -5)$		-8	-45	-27	-152
	$h_7=-3$				
$F_7=(-5,\ 7,\ 6)$		-45	$+143$	-152	$+483$

	-3	2	-1	1	-1	5	-3
$\frac{0}{1}$	$\frac{-1}{-3}$	$\frac{-2}{-7}$	$\frac{+3}{+10}$	$\frac{+5}{+17}$	$\frac{-8}{-27}$	$\frac{-45}{-152}$	$\frac{+143}{+483}$

Näherungswerthe von $\frac{\sqrt{79}-8}{3}$

	5	—1	1	—1	2	—3	5	Näherungswerthe
$\frac{1}{0}$	$\frac{+5}{-1}$	$\frac{-6}{+1}$	$\frac{-11}{+2}$	$\frac{+17}{-3}$	$\frac{+45}{-8}$	$\frac{-152}{+27}$	$\frac{-805}{+143}$	von $-\frac{\sqrt{79}+8}{3}$

Die dem mittleren Gliede F entsprechende Transformation $x = +1.x + 0.y$, $y = 0.x + 1.y$ ist nicht aus den vorstehenden Nebenrechnungen entnommen worden, sondern selbstständig gebildet; übrigens ist sie leicht zu verificiren, da sie die Form F, wie es sein muss, vollkommen unverändert lässt.

Da die Quotienten $\frac{\alpha_{-m}}{\gamma_{-m}}$, $\frac{\beta_{-m}}{\delta_{-m}}$ und $\frac{\alpha_m}{\gamma_m}$, $\frac{\beta_m}{\delta_m}$ sich bezüglich als zwei aufeinanderfolgende Näherungsbrüche zu den Ausdrücken $\frac{\sqrt{D}+b}{a}$ und $\frac{\sqrt{D}-b}{a}$ betrachten lassen, so ergeben sich aus der Theorie der Kettenbrüche unmittelbar folgende Eigenschaften derselben: 1) Sie gestatten keine Zurückführung auf kleinere Zahlen; 2) die absoluten Werthe der Zähler und Nenner nehmen mit wachsenden Indices beständig zu; 3) der Ausdruck $\frac{\sqrt{D}+b}{a}$ liegt zwischen den Werthen von $\frac{\alpha_{-m}}{\gamma_{-m}}$ und $\frac{\beta_{-m}}{\delta_{-m}}$ und der Ausdruck $\frac{\sqrt{D}-b}{a}$ liegt zwischen den Werthen von $\frac{\alpha_m}{\gamma_m}$ und $\frac{\beta_m}{\delta_m}$. Diese letzte Bemerkung führt zu dem folgenden Theoreme:

4) Wenn die reducirte Form $(a, b, -a')$ durch die Substitution $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$ in die gleichfalls reducirte und jener aequivalente Form $(A, B, -A')$ übergeht, so kann a entweder dasselbe Vorzeichen haben, wie die beiden Grössen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$, und dann ist die Quantität $\frac{\sqrt{D}-b}{a}$ zwischen den Brüchen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ enthalten und die reciproke Quantität $\frac{\sqrt{D}+b'}{a'}$ zwischen denselben aber umgekehrten Brüchen; oder a hat ein anderes Vorzeichen als die beiden Grössen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ und dann ist die Quantität $-\frac{\sqrt{D}+b}{a'}$ zwischen den Brüchen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ und die reciproke Quantität $-\frac{\sqrt{D}-b}{a}$ zwischen denselben aber umgekehrten Brüchen enthalten.

Zunächst bemerken wir, dass, wie es auch schon die Aussprüche des Theoremes voraussetzt, die Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ nothwendig von gleichem Zeichen sind. Denn da die beiden Formen $(a, b, -a')$ und $(A, B, -A')$ eigentlich aequivalent sind, so hat man die Bedingungsgleichung $\alpha\delta-\beta\gamma=1$ oder $\frac{\alpha}{\gamma}-\frac{\beta}{\delta}=\frac{1}{\gamma\delta}$ und damit diese erfüllt werden könne, ist offenbar nothwendig, dass die linke Seite eine wirkliche Differenz vorstelle, d. h. die Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ entweder beide zugleich positiv oder beide negativ sind.

Ferner ergiebt sich aus den bekannten Transformationsformeln

$$a\alpha^2+2b\alpha\gamma-a'\gamma^2=A,\quad a\beta^2+2b\beta\delta-a'\delta^2=-A'$$

durch Entwickelung der Quantitäten $\frac{\alpha}{\gamma}, \frac{\beta}{\delta}, \frac{\gamma}{\alpha}, \frac{\delta}{\beta}$

$$(1)\quad \frac{\alpha}{\gamma}=\frac{-b\pm\sqrt{D+\frac{aA}{\gamma^2}}}{a} \qquad (2)\quad \frac{\beta}{\delta}=\frac{-b\pm\sqrt{D-\frac{aA'}{\delta^2}}}{a}$$

$$(3)\quad \frac{\gamma}{\alpha}=\frac{+b\pm\sqrt{D-\frac{a'A}{\alpha^2}}}{a'} \qquad (4)\quad \frac{\delta}{\beta}=\frac{b\pm\sqrt{D+\frac{a'A'}{\beta^2}}}{a'}$$

Aus der Betrachtung dieser 4 Formeln fliesst unser Satz, der in zwei verschiedene Fälle zerfällt, von welchen jeder 2 verschiedene Aussagen umfasst:

a) Die Zahl *a* hat dasselbe Vorzeichen, wie die beiden Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\gamma}$. Dann sind $a.\frac{\alpha}{\gamma}$ und $a.\frac{\beta}{\delta}$ positive Grössen und darum in den Gleichungen (1) und (2) das untere Vorzeichen unstatthaft. Da nun $\sqrt{D}$ zwischen den in diesen Gleichungen enthaltenen Wurzelgrössen liegt (denn A und A' sind Grössen von dem nämlichen Zeichen), so muss $\frac{\sqrt{D}-b}{a}$ zwischen den beiden Brüchen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ enthalten sein und in weiterer Folge die zu $\frac{\sqrt{D}-b}{a}$ reciproke Quantität $\frac{\sqrt{D}+b}{a'}$ zwischen den beiden Brüchen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$.

b) Die Zahl a hat ein anderes Vorzeichen, als die beiden Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$ oder, was dasselbe sagt, als die beiden Brüche $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$. Dann sind die Producte $a'\frac{\gamma}{\alpha}$ und $a'.\frac{\delta}{\beta}$ beide negativ (denn a' und a haben gleiches Vorzeichen) und die Gleichungen (3) und (4) nur unter der Voraussetzung gültig, dass das untere Vorzeichen besteht. Lassen wir daher unter den beiden Wurzelzeichen daselbst die beiden Quantitäten $-\frac{a'A}{\alpha^2}$ und $+\frac{a'A'}{\beta^2}$ weg, die nothwendig verschiedenes Zeichen haben, so ergiebt sich die Quantität $\frac{-\sqrt{D}+b}{a'}$ als zwischen den Brüchen $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$ befindlich und in weiterer Folge liegt die zu $\frac{-\sqrt{D}+b}{a'}$ reciproke Quantität $\frac{-\sqrt{D}-b}{a}$ zwischen den Brüchen $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$.

In dem Beweise ist die stillschweigende Voraussetzung enthalten, dass, wenn der Fall *a*) eintritt, keine der Grössen α und β, und, wenn der Fall *b*) eintritt, keine der Grössen γ und δ sich annulliren. Thatsächlich kann aber keiner von diesen Umständen eintreten.

a) Wenn a ein anderes Vorzeichen hat, als die Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$, so kann weder α noch β sich annulliren.

Nehmen wir zuerst an, die Grösse α könnte gleich 0 werden: dann folgt aus der Gleichung $\alpha\delta-\beta\gamma=1$, dass man entweder $\beta=+1$ und $\gamma=-1$ oder $\beta=-1$ und $\gamma=+1$ habe. In beiden Fällen liefert die Gleichung $a\alpha^2+2b\alpha\gamma-a'\gamma^2=A$ den Werth $A=-a'$, d. h. die Zahlen A und a' haben entgegengesetztes Vorzeichen. Das Nämliche gilt darum auch von den Zahlen A' und a und die Grösse $-\frac{aA'}{\delta^2}$ ist demgemäss positiv. Nun erhellt, dass die Wurzelgrösse in (2) nur negativ genommen werden darf; denn im Falle des Gegentheils würden $\frac{\beta}{\delta}$ und a gleiches Zeichen haben, was gegen die Voraussetzung ist. Halten wir also das negative Vorzeichen fest, so folgt, wenn wir die positive Grösse $-\frac{aA'}{\delta^2}$ unter dem Wurzelzeichen vernachlässigen, in Rücksicht auf die absoluten Zahlenwerthe $\frac{\beta}{\delta}>\frac{\sqrt{D}-b}{a}$ oder, da wegen der Natur der zurückgebrachten Formen

die Grösse rechts vom Ungleichheitszeichen ein unächter Bruch ist, $\frac{\beta}{\delta} > 1$. Diese Ungleichung ist aber für ganzzahlige δ und für $\beta = \pm 1$ unmöglich.

Nehmen wir zweitens an, die Grösse β könnte gleich 0 werden, so würde aus der Ungleichung $\alpha\delta - \beta\gamma = +1$ folgen $\alpha = \pm 1$, $\delta = \pm 1$ und aus der Gleichung $a\beta^2 + 2b\beta\delta - a'\delta^2 = -A'$ der Werth $A' = a'$, so dass also auch A und a von demselben Zeichen und die Grösse $+\frac{aA}{\gamma^2}$ positiv sein müsste. Betrachten wir jetzt die Gleichung (3), so könnte sie nur für das untere Vorzeichen gelten, weil im entgegengesetzten Falle der Zähler rechts eine positive Grösse und daher $\frac{\alpha}{\gamma}$ und a von dem nämlichen Zeichen wären: aber auch diese Annahme ist unstatthaft: denn sie hat, durch Vernachlässigung der positiven Grösse $+\frac{aA}{\gamma^2}$ unter dem Wurzeichen die Ungleichung $\frac{\alpha}{\gamma} > \frac{-b-\sqrt{D}}{a}$ zu Folge, welche für ganzzahlige γ nicht bestehen kann, weil die Grösse rechts vom Ungleichheitszeichen ein unächter Bruch und $\alpha = \pm 1$ ist.

b) Wenn a dasselbe Vorzeichen hat, wie die Brüche $\frac{\gamma}{\alpha}$ und $\frac{\delta}{\beta}$, so kann weder γ noch δ sich annulliren.

Die Annahme $\gamma = 0$ führt auf die Gleichungen $\alpha = \pm 1$, $\delta = \pm 1$, $a = A$ und, durch Zuziehung von (4), auf die sich widersprechende Ungleichung $\frac{\delta}{\beta} > 1$.

Die zweite Annahme $\delta = 0$ führt auf die Gleichungen $\beta = \pm 1$, $\gamma = \mp 1$, $-A' = a$ und, durch Zuziehung von (3), auf die sich widersprechende Ungleichung $\frac{\gamma}{\alpha} > 1$.

Es wird gut sein ausdrücklich zu bemerken, dass, wenn a ein anderes Vorzeichen hat, als die beiden Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$, zwar keine der Grössen α und β, wohl aber eine der Grössen γ und δ sich annulliren kann, und dass, wenn a dasselbe Vorzeichen hat, wie die beiden Brüche $\frac{\alpha}{\gamma}$ und $\frac{\beta}{\delta}$, zwar keine der Grössen γ und δ, wohl aber eine der Grössen α und β sich annulliren kann: in beiden speciellen Fällen behält das

obige Theorem seine Gültigkeit. Betrachten wir z. B. die beiden angrenzenden Formen $(a, b, -a')$, $(A, B, -A')$ unter der Voraussetzung, dass a eine positive Grösse und $A = -a'$ sei, so hat man $x = 0 . X - 1 . Y$, $y = 1 . x - \frac{b+B}{a'}$, also $\frac{\alpha}{\gamma} = \frac{0}{1}$, $\frac{\beta}{\delta} = \frac{a'}{b+B}$, d. h. beide Brüche positiv, wie die Grösse a; demgemäss folgen die beiden Ungleichungen $0 < \frac{\sqrt{D}-b}{a} < \frac{a'}{b+b'}$ und $\frac{b+b'}{a'} < \frac{\sqrt{D}+b}{a'} < \infty$, welche leicht zu verificiren sind, wenn man bedenkt, dass $\sqrt{D} > b$ und $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$ ist.

Vermittelst des eben bewiesenen Theoremes sind wir nun im Stande folgenden Hauptsatz zu beweisen, auf welchen, wie schon bei einer früheren Gelegenheit, wir in diesem Paragraphen verwiesen haben:

Wenn zwei zurückgebrachte Formen einander im eigentlichen Sinne aequivalent sind, so ist eine jede von ihnen in der Periode der anderen enthalten.

Behufs des Beweises ist es indessen zweckmässig noch einen zweiten Hülfssatz einzuschieben, nämlich den folgenden: Wenn die Gleichung $mn' + m'n = \mp 1$ besteht, so ist der Nenner jedes der beiden Brüche $\frac{m}{n}$ und $\frac{m'}{n'}$ kleiner als der Nenner irgend eines beliebig zwischen diesen eingeschobenen Bruches $\frac{\mu}{\nu}$. — Zu Folge der Voraussetzung liegt $\mu nn'$ zwischen $\nu mn'$ und $\nu m'n$ und man hat daher, absolut genommen, $\nu mn' - \nu m'n = \nu(mn' - m'n) = \mp \nu > \nu mn' - \mu nn'$ und auch $> \nu m'n - \mu nn'$. Diese beiden Ungleichungen lassen sich umformen, wie folgt: $\nu > n'(\nu m - \mu n)$ und $\nu > n(\nu m' - \mu n')$ und da die beiden Quantitäten $\nu m - \mu n$ und $\nu m' - \mu n'$ auf jeden Fall von 0 verschiedene ganze Zahlen sind (denn wäre eine dieser Quantitäten gleich 0, so hätte man $\frac{\mu}{\nu} = \frac{m}{n}$ oder $\frac{\mu}{\nu} = \frac{m'}{n'}$, d. h. der Bruch $\frac{\mu}{\nu}$ wäre nicht zwischen $\frac{m}{n}$ und $\frac{m'}{n'}$ eingeschoben, sondern fiele mit einem der beiden Grenzwerthe zusammen), so gelten um so stärker die beiden Ungleichungen $\nu > n'$, $\nu > n$, welche zu beweisen sind.

Seien jetzt $(a, b, -a')$ und $(A, B, -A')$ zwei im eigentlichen Sinne aequivalente Formen und gehe die erste in die zweite über durch die

Substitutionen $x = \alpha' X + \beta' Y$, $y = \gamma' X + \delta' Y$. Bilden wir uns die zu der Form $f = (a, b, -a'$ gehörige Periode und denken wir uns die aufeinanderfolgenden Transformationen von f in die verschiedenen Formen dieser Periode berechnet, wie es in dem nachfolgenden Schema sich angedeutet findet:

$$\begin{array}{llll} \ldots\ldots (a_{-2}, b_{-2}, -a_{-1}) & (-a_{-1}, b_{-1}, a) & (a, b, -a') & (-a', b', a'') \\ \ldots\ldots \quad \alpha_{-2}\beta_{-2}\gamma_{-2}\delta_{-2} & \alpha_{-1}\beta_{-1}\gamma_{-1}\delta_{-1} & & \alpha_1\beta_1\gamma_1\delta_1 \\ & & & (a'', b'', -a''') \ldots\ldots \\ & & & \alpha_2\beta_2\gamma_2\delta_2 \quad \ldots\ldots \end{array}$$

Dann wollen wir darthun, dass irgend ein Coefficient der gegebenen Transformation, z. B. α', dem gleichnamigen Coefficienten α_m irgend einer speciellen Transformation des Schemas gleich sei und dass man in Folge hiervon $\beta' = \beta_m$, $\gamma' = \gamma_m$, $\delta' = \delta_m$ habe, oder dass $\alpha' = -\alpha_m$ und in Folge hiervon $\beta' = -\beta_m$, $\gamma' = \gamma_m$, $\delta' = -\delta_m$ sei: in beiden Fällen sind die Formen F und f_m identisch und der Satz daher bewiesen.

Um zum Zwecke zu gelangen bemerken wir, dass zu Folge der Voraussetzung folgende Transformationsformeln bestehen:

$$(1) \quad a\alpha'^2 + 2b\alpha'\gamma' - a'\gamma'^2 = A \qquad (3) \quad a\beta'^2 + 2b\beta'\delta' - a'\delta'^2 = -A'$$

$$(2) \quad a\alpha'\beta' + b(\alpha'\delta' + \beta'\gamma') - a'\gamma'\delta' = B$$

$$(4) \quad \alpha\delta - \beta\gamma = +1.$$

Erster Fall. Die Zahl a hat dasselbe Vorzeichen, wie die beiden Brüche $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$. Alsdann kann weder γ' noch δ' gleich 0 sein, wohl aber α oder β; wir bekommen daher zwei Nebenfälle, die den Annahmen $\alpha' = 0$ und $\beta' = 0$ entsprechen und einen Hauptfall, in welchem die 4 Grössen α', β', γ', δ' alle von 0 verschieden sind.

a) Sei zunächst $\alpha' = 0$, so folgt aus (4) $\beta' = \pm 1$, $\gamma' = \mp 1$, aus (1) $-a' = A$ und aus (2) $-b \pm a'\delta = B$, d. h. $B + b \equiv 0 \pmod{a'}$. Demgemäss ist die Form $(a, b, -a')$ in Bezug auf ihre letzte Partie der reducirten Form $(A, B, -A')$ angrenzend und muss daher nach dem Theoreme unter 1) *d*) in diesem §. nothwendig mit F_1 identisch sein: d. h. man hat $\alpha' = \alpha_1 = 0$, $\beta' = \beta_1 = -1$, $\gamma' = \gamma_1 = 1$, $\delta' = \delta_1 = h_1$.

b) Sei $\beta' = 0$, dann wird aus (4) $\alpha = \pm 1$, $\delta = \pm 1$, aus (3) $a' = A'$ und aus (2) $b - a'\gamma' = B$ oder $b \equiv B \pmod{a'}$. Nun liegen sowohl b, wie B, weil die Formen $(a, b, -a')$ und $(A, B, -A')$ beide reducirte

sind, zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-a'$, darum ist nothwendig $b=B$ und daher endlich wegen Gleichheit der Determinanten $a'=A'$; d. h. die Formen f und F sind identisch.

c) Wir nehmen endlich die 4 Grössen α, β, γ, δ, alle als von 0 verschieden an.

Da die Brüche $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$ dasselbe Zeichen haben, wie a, so liegt die Quantität $\frac{\sqrt{D}-b}{a}$, welche wir der Kürze halber mit L bezeichnen wollen, nach dem Anfangstheoreme dieser Nummer zwischen $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$; ordnen wir diese drei Grössen nach der absoluten Grösse und nehmen wir an, dass wir dadurch folgende Reihe bekämen:

$$(5)\qquad \frac{\beta'}{\delta'}\quad L\quad \frac{\alpha'}{\gamma'}.$$

(Die umgekehrte Ordnung würde in dem Wesen des Beweises keine Aenderung hervorbringen). Nun ist, wie wir wissen, die Quantität L auch noch zwischen je zwei aufeinanderfolgenden Näherungswerthen enthalten, also zwischen den absoluten Werthen von $\frac{\alpha_1}{\gamma_1}$ und $\frac{\alpha_2}{\gamma_2}$, $\frac{\alpha_2}{\gamma_2}$ und $\frac{\alpha_3}{\gamma_3}$, $\frac{\alpha_3}{\gamma_3}$ und $\frac{\alpha_4}{\gamma_4}$ ....., und da die Brüche $\frac{\alpha_m}{\gamma_m}$ mit wachsenden Indices näher an L heranrücken, so können wir nun die zweite mit dem Gliede $\frac{\alpha_1}{\gamma_1}=0$ beginnende Reihe aufsteigender Grössen bilden:

$$(6)\qquad \frac{\alpha_1}{\gamma_1}\quad \frac{\alpha_3}{\gamma_3}\quad \frac{\alpha_5}{\gamma_5}\quad \ldots\ldots\quad L\quad \ldots\ldots\quad \frac{\alpha_6}{\gamma_6}\quad \frac{\alpha_4}{\gamma_4}\quad \frac{\alpha_2}{\gamma_2}.$$

Es kommt jetzt darauf an zu beweisen, dass $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$ irgend zwei aufeinanderfolgenden Gliedern der Reihe (6) gleich werden. Zunächst erhellt, dass sie beide als von 0 verschieden rechts von $\frac{\alpha_1}{\gamma_1}$ liegen müssen. Also $\frac{\beta'}{\delta'}$ liegt rechts von $\frac{\alpha_1}{\gamma_1}$ und links von L. Was nun die andere Grösse $\frac{\alpha'}{\gamma'}$ betrifft, so liegt dieselbe nothwendig rechts von L, aber nicht rechts über $\frac{\alpha_2}{\gamma_2}$ hinaus. Unter dieser Annahme nämlich hätten wir die steigende Reihe $\frac{\alpha_1}{\gamma_1}$, $\frac{\beta'}{\delta'}$, L, $\frac{\alpha_2}{\gamma_2}$, $\frac{\alpha'}{\gamma'}$ und wir hätten, indem die Bedingung $\alpha_1\gamma_2-\alpha_2\gamma_1=\pm 1$

erfüllt würde, $\frac{\beta'}{\delta'}$ zwischen den beiden Brüchen $\frac{\alpha_1}{\gamma_1}$ und $\frac{\alpha_2}{\gamma_2}$ und gleichzeitig, indem die Bedingung $\beta'\gamma' - \alpha'\delta' = 1$ erfüllt wird, $\frac{\alpha_2}{\gamma_2}$ zwischen den beiden Brüchen $\frac{\beta'}{\delta'}$ und $\frac{\alpha'}{\gamma'}$. Daraus würden sich aber nach unserem vorausgeschickten Hülfssatze die beiden einander widersprechenden Ungleichungen $\delta' > \gamma_2$ und $\delta' < \gamma_2$ ergeben. Also liegt $\frac{\alpha'}{\gamma'}$ auf keinen Fall rechts von $\frac{\alpha_2}{\gamma_2}$ und ist mithin entweder ein Glied der Reihe rechts von L oder es liegt wenigstens zwischen zwei aufeinanderfolgenden Gliedern. Seien diese Glieder $\frac{\alpha_{2m}}{\gamma_{2m}}$ und $\frac{\alpha_{2m+2}}{\gamma_{2m+2}}$: dann kann man darthun, dass $\frac{\beta'}{\delta'}$ geradezu gleich wird dem der Grösse nach zwischen jenen liegenden Gliede $\frac{\alpha_{2m+1}}{\gamma_{2m+1}}$. Käme nämlich $\frac{\beta'}{\delta'}$ nicht geradezu auf das letztgenannte Glied zu liegen, so müsste es entweder rechts oder links davon liegen und es würden diesen beiden Annahmen respective die beiden aufsteigenden Reihen entsprechen:

$$\frac{\alpha_{2m+1}}{\gamma_{2m+1}} \quad \frac{\beta'}{\delta'} \quad L \quad \frac{\alpha_{2m+2}}{\gamma_{2m+2}} \quad \frac{\alpha'}{\gamma'} \quad \frac{\alpha_{2m}}{\gamma_{2m}},$$

$$\frac{\beta'}{\delta'} \quad \frac{\alpha_{2m+1}}{\gamma_{2m+1}} \quad L \quad \frac{\alpha_{2m+2}}{\gamma_{2m+2}} \quad \frac{\alpha'}{\gamma'} \quad \frac{\alpha_{2m}}{\gamma_{2m}}.$$

Die erste Reihe ergiebt, weil sowohl $\frac{\beta'}{\delta'}$ zwischen $\frac{\alpha_{2m+1}}{\gamma_{2m+1}}$ und $\frac{\alpha_{2m+2}}{\gamma_{2m+2}}$, wie auch $\frac{\alpha_{2m+2}}{\gamma_{2m+2}}$ zwischen $\frac{\beta'}{\delta'}$ und $\frac{\alpha'}{\gamma'}$ läge, die beiden einander widersprechenden Ungleichungen $\delta' > \gamma_{2m+2}$ und $\gamma_{2m+2} > \delta'$; die zweite Reihe ergiebt, weil sowohl $\frac{\alpha_{2m+1}}{\gamma_{2m+1}}$ zwischen $\frac{\beta'}{\delta'}$ und $\frac{\alpha'}{\gamma'}$, wie auch $\frac{\alpha'}{\gamma'}$ zwischen $\frac{\alpha_{2m+1}}{\gamma_{2m+1}}$ und $\frac{\alpha_{2m}}{\gamma_{2m}}$ läge, die beiden gleichfalls einander widersprechenden Ungleichungen $\gamma_{2m+1} > \gamma'$ und $\gamma' > \gamma_{2m+1}$. Also ist der absolute Werth von $\frac{\beta'}{\delta'}$ identisch mit dem absoluten Werthe von $\frac{\alpha_{2m+1}}{\gamma_{2m+1}}$. Nun sind beide Brüche in den kleinsten Zahlen ausgedrückt; denn wegen der Gleichungen $\alpha'\delta' - \beta'\gamma' = 1$ und $\alpha_{2m}\gamma_{2m+1} - \alpha_{2m+1}\gamma_{2m} = \pm 1$ sind sowohl β' und δ', wie auch α_{2m+1} und γ_{2m+1} relative Primzahlen zu einander. Die eben erwähnte Identität

kann daher nur bestehen, entweder wenn $\beta' = \alpha_{2m+1}$, $\delta' = \gamma_{2m+1}$ oder $\beta' = -\alpha_{2m+1}$, $\delta' = -\gamma_{2m+1}$ ist.

Wir haben bis jetzt dargethan, dass entweder $\frac{\alpha'}{\gamma'}$ mit irgend einem Gliede der Reihe zwischen $\frac{\alpha_1}{\gamma_1}$ und L zusammenfällt, etwa mit $\frac{\alpha_{2m}}{\gamma_{2m}}$ oder, wenn $\frac{\alpha_1}{\gamma_1}$ als nicht unmittelbar mit einem Gliede zusammenfallend angenommen wird, gerade diese Annahme die Gleichheit von $\frac{\beta'}{\delta'}$ und $\frac{\alpha_{2m+1}}{\gamma_{2m+1}}$ zu Folge hat und mithin $\beta' = \pm\alpha_{2m+1}$, $\delta' = \pm\gamma_{2m+1}$ ist. Vergleichen wir in dem letzten Falle die Transformation von f in F mit der Transformation von f in f_{2m}, so erhalten wir $\alpha' = \pm\alpha_{2m}$, $\gamma' = \pm\gamma_{2m}$ und die Formen F und f_{2m} sind daher identisch. Eben diese Formen ergeben sich auch in dem ersten Falle als identisch und das Theorem ist daher für den ersten Hauptfall vollständig bewiesen.

Die Transformation von f in f_{2m} hat zu Folge die Gleichungen:

$$(7)\quad a\alpha_{2m}^2 + 2b\alpha_{2m}\gamma_{2m} - a'\gamma_{2m}^2 = \pm a_{2m}$$

$$(8)\quad a\beta_{2m}^2 + 2b\beta_{2m}\delta_{2m} - a'\delta_{2m}^2 = \mp a_{2m+1}$$

$$(9)\quad a\alpha_{2m}\beta_{2m} + b(\alpha_{2m}\delta_{2m} + \beta_{2m}\gamma_{2m}) - a'\gamma_{2m}\delta_{2m} = b_{2m}$$

$$(10)\quad \alpha_{2m}\delta_{2m} - \beta_{2m}\gamma_{2m} = 1.$$

Substituiren wir in die Gleichung (10) für β_{2m} den Werth $\delta_{2m+1} = \pm\beta'$ und für δ_{2m} den Werth $\alpha_{2m+1} = \pm\delta'$, so geht sie über in $\alpha_{2m}\delta' - \gamma_{2m}\beta' = \pm 1$ und indem wir, wenn das obere Vorzeichen gilt, die Gleichung (4) hiervon subtrahiren, dagegen, wenn das obere Vorzeichen gilt, die Gleichung (4) dazu addiren, bekommen wir $\delta'(\alpha_{2m} \mp \alpha') - \beta'(\gamma_{2m} \mp \gamma') = 0$ oder $\frac{\alpha_{2m} \mp \alpha}{\gamma_{2m} \mp \gamma'} = \frac{\beta'}{\delta'}$ und hieraus folgt, wenn wir annehmen, dass r der grösste gemeinschaftliche Theiler zwischen Nenner und Zähler des Bruches links ist, $\alpha_{2m} = r\beta' \pm \alpha'$, $\gamma_{2m} = r\delta' + \gamma'$. Substituirt man jetzt für α_{2m}, β_{2m}, γ_{2m}, δ_{2m} in der Gleichung (9) ihre Werthe $r\beta' \pm \alpha'$, $\pm\beta'$, $r\delta' + \gamma'$, $\pm\delta'$, so bekommen wir $a(r\beta' \pm \alpha') \,.\, \pm\beta' + b\left\{(r\beta' + \alpha') \,.\, \pm\delta' + (r\delta' \pm \gamma') \,.\, \pm\beta'\right\} - a'(r\delta' \pm \gamma') \,.\, \pm\delta' = b_{2m}$ oder, wenn man entwickelt

$$\pm r(a\beta'^2 + 2b\beta'\delta' - a'\delta'^2) + \left\{a\alpha'\beta' + b(\alpha'\delta' + \beta'\gamma') - a'\gamma'\delta'\right\} = b_{2m}$$

oder endlich, wenn man für die eingeklammerten Grössen ihre Werthe aus (3) und (2) substituirt, $\mp rA' + B = b_{2m}$ oder $B \equiv b_{2m}\ (mod\ A')$, wo

der Modul A' natürlich nur als absolute Zahl zu denken ist. Nun liegen B und b_{2m} beide zwischen den nämlichen Grenzen $\sqrt{D}$ und $\sqrt{D}-[A']$. Betreffs der Grösse B folgt dies unmittelbar daraus, dass die Form F eine reducirte ist; dagegen die Grösse b_{2m} liegt zunächst zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D}-[a_{2m+1}]$, aber man hat $A'=\pm a_{2m+1}$: denn die Einsetzung von $\pm\beta'$ und $\pm\delta'$ für β_{2m} und δ_{2m} in (8) liefert die Gleichung $a\beta'^2+2b\beta'\delta'-a'\delta'^2=\mp a_{2m+1}$, aus welcher durch Vergleichung mit der Gleichung (3) die behauptete Gleichheit folgt. Also kann die genannte Congruenz nur bestehen unter der Annahme $B=b_{2m}$. Diese letzte Gleichung in Verbindung mit der eben erwähnten $A'=\pm a_{2m+1}$ hat die dritte Gleichung $A=\pm a_{2m}$ zu Folge und die beiden Formen F und f_{2m} sind daher identisch.

Der eben geführte Beweis gilt unter der Annahme (die beiläufig mit ihm als eine illusorische zusammenfällt), dass $\frac{\alpha'}{\gamma'}$ sich nicht unmittelbar als mit einem Gliede der Reihe (6) identisch zeige. Nehmen wir nun im Gegentheile an, es fiele unmittelbar mit dem Gliede $\frac{\alpha_{2m}}{\gamma_{2m}}$ zusammen, so lässt sich die Identität der Formen F und f_{2m} gleichfalls nachweisen. Man hat alsdann $\alpha_{2m}=\pm\alpha'$, $\gamma_{2m}=\pm\gamma'$ und diese Werthe in (7) eingesetzt bekommt man durch Vergleichung mit (1) die Gleichheit $A=\pm a_{2m}$. Ferner liefert ein ähnlicher Calcül, wie der vorhergehende, die Gleichung $\pm rA+B=b_{2m}$ oder $B\equiv b_{2m}$ (*mod* A) und da B und b_{2m} wieder zwischen den nämlichen Grenzen $\sqrt{D}$ und $\sqrt{D}-[A]$ liegen, zwischen denen nur eine einzige particuläre Lösung enthalten ist, so geht die Congruenz über in die Gleichheit $B=b_{2m}$. Da jetzt die beiden Formen F und f_{2m} die beiden ersten Coefficienten gleich und ausserdem die Determinanten gleich haben, so sind sie identisch.

Wir bemerken noch, dass in beiden Fällen nothwendig $r=0$ sein muss, im ersten Falle, weil die Gleichungen $\mp rA'+B=b_{2m}$ und $B=b_{2m}$, und im zweiten Falle, weil die Gleichungen $\pm rA+B=b_{2m}$ und $B=b_{2m}$ zusammen bestehen. Damit wird $\alpha_{2m}=\pm\alpha'$, $\beta_{2m}=\pm\beta'$, $\gamma_{2m}=\pm\gamma'$, $\delta_{2m}=\pm\delta'$ oder mit andern Worten: die Transformation von f in F findet sich unter der Reihe der auf f bezüglichen Transformationen irgendwo vor.

Zweiter Fall. Die Zahl a hat ein anderes Vorzeichen als die beiden Brüche $\frac{\alpha'}{\gamma'}$ und $\frac{\beta'}{\delta'}$. Alsdann kann weder α' noch β' gleich 0 sein, wohl aber γ' und δ'. Wir bekommen daher zwei Nebenfälle, die den Annahmen $\gamma' = 0$ und $\delta' = 0$ entsprechen und einen Hauptfall, in welchem die 4 Grössen α', β', γ', δ' alle von 0 verschieden sind.

a) Sei zunächst $\gamma' = 0$, so folgt aus (4) $\alpha' = \pm 1$, $\delta' = \pm 1$, aus (1) $a = A$ und aus (2) $b \equiv B \pmod a$; also, da b und B beide zwischen den Grenzen $\sqrt{D}$ und $\sqrt{D} - [a]$ liegen, wird $b = B$ und die beiden Formen f und F sind identisch.

b) Sei $\delta' = 0$, so folgt aus (4) $\beta' = \pm 1$, $\gamma' = \mp 1$, aus (3) $a = -A'$ und aus (2) $b + B \equiv 0 \pmod a$, also sind die beiden Formen f und F angrenzende und daher wird F nothwendig identisch mit $f_{-1} = (-a_{-1}, b_{-1}, a)$.

c) Wir nehmen endlich die 4 Grössen α, β, γ, δ alle als von 0 verschieden an.

Da die Brüche $\frac{\gamma'}{\alpha'}$ und $\frac{\delta'}{\beta'}$ ein anderes Zeichen haben als a, so liegt nach dem diese Nummer einleitenden Theorem die Quantität $\frac{-\sqrt{D}+b}{a'}$, welche wir der Kürze halber mit L' bezeichnen, zwischen den Brüchen $\frac{\gamma'}{\alpha'}$ und $\frac{\delta'}{\beta'}$. Ordnen wir nun diese drei Quantitäten nach ihrer absoluten Grösse und nehmen an, wir bekämen dadurch folgende aufsteigende Reihe (in der die Glieder nur nach ihrer absoluten Grösse gelten):

$$(11)\quad \frac{\gamma'}{\alpha'} \quad L' \quad \frac{\delta'}{\beta'}$$

(die umgekehrte Ordnung, wenn sie factisch eintreten sollte, würde in dem Wesen des Beweises nichts ändern). Nun ist, wie wir wissen, die Quantität L' auch noch zwischen je zwei ihrer aufeinanderfolgenden Näherungswerthe enthalten, also zwischen den (absoluten) Werthen von $\frac{\delta}{\beta}$, $\frac{\delta_{-1}}{\beta_{-1}}$, $\frac{\delta_{-2}}{\beta_{-2}}$, $\frac{\delta_{-3}}{\beta_{-3}}$, ... und da dieselben mit wachsenden Indices immer näher an L' heranrücken, so hat man, wenn man bedenkt, dass $\frac{\delta}{\beta} = 0$ ist, die aufsteigende Reihe:

$$(12)\quad \frac{\delta}{\beta} \quad \frac{\delta_{-2}}{\beta_{-2}} \quad \frac{\delta_{-4}}{\beta_{-4}} \quad \ldots\ldots \quad L' \quad \ldots\ldots \quad \frac{\delta_{-5}}{\beta_{-4}} \quad \frac{\delta_{-3}}{\beta_{-3}} \quad \frac{\delta_{-1}}{\beta_{-1}}.$$

Was nun die Grösse $\frac{\gamma'}{\alpha'}$ betrifft, so muss sie nothwendig rechts von $\frac{\delta}{\beta}$ und links von L' liegen, so dass sie entweder mit einem dazwischen gelegenen Gliede zusammenfällt oder zwischen zwei aufeinanderfolgenden sich befindet. Die andere Grösse $\frac{\delta'}{\beta'}$ dagegen liegt rechts von L', aber nicht rechts über $\frac{\delta_{-1}}{\beta_{-1}}$ hinaus. Diese Annahme nämlich würde die folgende aufsteigende Reihe ergeben:

$$\frac{\delta}{\beta} \quad \frac{\gamma'}{\alpha'} \quad L' \quad \frac{\delta_{-1}}{\beta_{-1}} \quad \frac{\delta'}{\beta'}$$

und es würden, weil sowohl $\frac{\gamma'}{\alpha'}$ zwischen $\frac{\delta}{\beta}$ und $\frac{\delta_{-1}}{\beta_{-1}}$ mit der Bedingung $\delta\beta_{-1} - \beta\delta_{-1} = -1$, wie auch $\frac{\delta_{-1}}{\beta_{-1}}$ zwischen $\frac{\delta'}{\beta'}$ und $\frac{\gamma'}{\alpha'}$ mit der Bedingung $\delta'\alpha' - \beta'\gamma' = +1$ läge, die beiden sich widersprechenden Ungleichungen $\alpha' > \beta_{-1}$ und $\beta_{-1} > \alpha'$ folgen. Also ist $\frac{\delta'}{\beta'}$ entweder ein Glied der Reihe von L' bis zu $\frac{\delta_{-1}}{\beta_{-1}}$ oder es liegt zwischen irgend welchen zwei aufeinanderfolgenden Gliedern. Seien diese Glieder $\frac{\delta_{-2m-1}}{\beta_{-2m-1}}$ und $\frac{\delta_{-2m+1}}{\beta_{-2m+1}}$, so lässt sich wie vorhin zeigen, dass $\frac{\gamma'}{\alpha'}$ weder links noch rechts von $\frac{\delta_{-2m}}{\beta_{-2m}}$ liegen kann und darum mit dem letztgenannten Bruche identisch ist.

Der weitere Beweis nimmt genau den nämlichen Gang, wie im ersten Falle und hat zum Endresultate die Identität der Formen F und f_{-2m}.

Betrachten wir irgend zwei uneigentlich aequivalente und reducirte Formen F und f und nennen die mit F associirte und ihr daher gleichfalls uneigentlich aequivalente Form F': dann sind die beiden Formen F' und f einander im eigentlichen Sinne aequivalent und demzufolge die Form F' in der Periode der Form f mit enthalten. Sind nun die beiden Formen F und f sowohl eigentlich, wie uneigentlich aequivalent, so ist gleichzeitig auch noch F in der Periode der Form f enthalten. Darum ist die Periode mit sich selber associirt und muss daher zwei zweideutige Formen in sich schliessen. Da nun alle Formen einer Periode einander eigentlich aequivalent sind; so erhellt das Theorem:

Wenn zwei Formen einander sowohl eigentlich, wie uneigentlich aequivalent sind, so kann immer eine zweideutige Form gefunden werden, welche beiden aequivalent ist.

Die beiden Formen des Theoremes brauchen, wie man leicht sieht, nicht gerade reducirte zu sein. Auch gilt der Satz gleichmässig für eine positive, wie für eine negative Determinante.

5) Seien jetzt zwei beliebige Formen $\Phi = (A, B, A')$ und $\varphi = (a, b, a')$ mit positiver Determinante gegeben, so kann man immer entscheiden, ob sie einander aequivalent sind oder nicht.

Man suche zu beiden die reducirten Formen F und f, die den vorgelegten nothwendig aequivalent sind, und entwickele sich die zu irgend einer von ihnen gehörige Periode, etwa die Periode von f. Nun können folgende vier Fälle eintreten: 1) Die Periode von f enthält weder die Form F, noch die ihr associirte: dann sind Φ und φ weder eigentlich, noch uneigentlich aequivalent. 2) Die Periode von f enthält die Form F, aber nicht die ihr associirte: dann sind die Formen Φ und φ im eigentlichen und nur im eigentlichen Sinne aequivalent. 3) Die Periode von f enthält zwar nicht die Form F, wohl aber die ihr associirte: dann sind die Formen Φ und φ im uneigentlichen und nur im uneigentlichen Sinne aequivalent. 4) Die Periode von f enthält sowohl die Form F, wie auch die ihr associirte: dann sind die Formen Φ und φ sowohl im eigentlichen, wie im uneigentlichen Sinne aequivalent.

An dieses Problem knüpft sich das nachfolgende an: Wenn zwei im eigentlichen Sinne aequivalente Formen Φ und φ gegeben sind, eine Transformation der einen in die andere aufzufinden.

Man bilde sich zunächst unter Anwendung der im Anfange dieses Paragraphen auseinandergesetzten Methode die auf Φ bezügliche Reihe der angrenzenden Formen:

$$(1) \quad \Phi,\ \Phi',\ \Phi'',\ \Phi''',\ \ldots\ldots\ \Phi^{(n-1)},\ \Phi^{(n)},$$

welche mit der ersten reducirten Form $\Phi^{(n)}$ zu Φ schliessen möge. Darauf bilde man sich die entsprechende auf φ bezügliche Reihe, schliesse dieselbe aber nicht mit der ersten reducirten Form $\varphi^{(\nu)}$, sondern setze sie noch weiter fort, bis man, was wegen der Aequivalenz der reducirten

Formen $\Phi^{(n)}$ und $\varphi^{(n)}$ nothwendig irgend einmal eintreten muss, zu der Form $\Phi^{(n)}$ gelangt, so dass die zweite Reihe folgende Gestalt erhält:

$$(2)\quad \varphi,\ \varphi',\ \varphi'',\ \ldots\ldots\ \varphi^{(\nu)},\ \varphi^{(\nu+1)},\ \varphi^{(m-2)},\ \varphi^{(m-1)},\ \Phi^{(n)}.$$

Bilden wir uns nun zu den aufeinanderfolgenden Formen der ersten Reihe die associirten und dazu die entgegengesetzten, so erhalten wir die folgende dritte Reihe angrenzender Formen:

$$(3)\quad \psi,\ \psi',\ \psi'',\ \ldots\ldots\ \psi^{(n-1)},\ \psi^{(n)}$$

und können (der Beweis ist ähnlich wie im vorigen Paragraphen bei der entsprechenden Aufgabe) die zweite und dritte Reihe zu der einzigen Reihe von angrenzenden Formen zusammensetzen:

$$(4)\quad \varphi,\ \varphi',\ \varphi'',\ \varphi''',\ \ldots\ldots\ \varphi^{(\nu)},\ \varphi^{(\nu+1)},\ \ldots\ldots\ \varphi^{(m-1)},\ \psi^{(n-1)},\ \psi^{(n-2)}\ \ldots\ldots\ \psi',\ \psi,\ \Phi.$$

Vermittelst dieser letzten Reihe kann man eine Transformation der Form φ in die Form Φ vermöge der in §. 22 unter 3) auseinandergesetzten Methode herleiten.

Die Möglichkeit diese Transformation auszuführen giebt nun das Mittel an die Hand zur Lösung des fundamentalen Theoremes, welches der Zielpunkt unserer ganzen Discussion ist: Solche specielle Zahlenwerthe von x und y zu bestimmen, für welche die Form (A, B, C) mit positiver Determinante D eine gegebene Zahl repräsentirt oder mit anderen Worten die Gleichung

$$Ax^2 + 2Bxy + Cy^2 = M$$

in relativen Primzahlen für x und y aufzulösen.

Die Auflösung ist vollständig analog der Auflösung desselben Problemes für eine negative Determinante, welche am Schlusse des vorhergehenden Paragraphen ist und wirklich auch für den in Rede stehenden Fall einer positiven und nicht quadratischen Determinante passt; wir haben daher wohl nicht nöthig uns hier weiter darüber zu verbreiten. Auch die an der angeführten Stelle weiterhin folgenden Betrachtungen (insbesondere über solche Lösungen in x und y, die keine relativen Primzahlen sind) greifen eben so sehr für eine positive, wie für eine negative Determinante Platz. Wir begnügen uns demgemäss ein durchgerechnetes Beispiel folgen zu lassen.

Beispiel. Die vorgelegte Gleichung sei $4x^2+28xy+20y^2 = 956$, also $D = 116$ und $\sqrt{D}$ zwischen 10 und 11. Die Hülfsgleichung wird

$z^2 - 116 = 956s$ oder, wenn man $4s = u - 1$ setzt, um eine Gleichung von der Form $x^2 + r = Pu$ zu gewinnen, in der r und P positiv und r unterhalb P ist, $z^2 + 123 = 239u$. Vermöge der am Schlusse von §. 20 auseinandergesetzten Methode und unter Beibehaltung der dortigen Bezeichnung findet man $239.3 = 15^2 + 2^2.123$, also $2n+1 = 15$, $n = 7$, $n^2 + r = 172$, $u = 516$, $z = \pm 351$. Hiernach zu Folge der Formeln von §. 19 oder auch vermittelst der Theorie der Congruenzen findet man nach der absoluten Grösse geordnet folgende Reihe zusammengehöriger Werthe von z und u: $z = \pm 112$, $u = 53$; $z = \pm 127$, $u = 68$; $z = \pm 351$, $u = 516$; $z = \pm 366$, $u = 561$; $z = \pm 590$, $u = 1457$; ...... Da man nun die Gleichung $4s = u - 1$ hat, so suche man, um alle nur möglichen Lösungen der Gleichung $z^2 - 116 = 956s$, die von einander wesentlich verschieden und in den kleinsten Zahlen ausgedrückt sind, zu erhalten, diejenigen unter den vorstehenden Lösungssystemen in z und u, für welche $z \leqq \frac{956}{2} = 478$ ist und $u - 1$ durch 4 ohne Rest getheilt werden kann. Wir bekommen auf diese Weise die 4 Werthsysteme:

$$z = +112,\ s = 13;\ z = -112,\ s = 13;\ z = +366,\ s = 140;$$
$$z = -366,\ s = 140,$$

und in der That giebt es nicht mehr, denn $956 = 2^2.239$ und hat daher nicht mehr als 2 von einander verschiedene Primfactoren.

Jedes dieser 4 Lösungssysteme kann möglicher Weise zu irgend einer speciellen Repräsentation der Zahl 956 durch die gegebene Form gehören und wir müssen daher dieselben alle untersuchen. Wir wollen die Rechnung zuerst an dem dritten durchführen und vergleichen demgemäss die beiden Formen (4, 14, 20) und (956, 366, 140). Diese Vergleichung führt folgende Rechnung herbei:

$(4, 14, 20)$; $10 \geqq b > 10 - 20$, $14 + b = 20h$, $b = 6$, $h = 1$,
$a' = 4 - (14 - 6) = -4$

$(20, 6, -4)$; $10 \geqq b > 10 - 4$, $6 + b = -4h$, $b = 2$, $h = -2$,
$a' = 20 + 2(6 - 2) = 28$

$(-4, 2, 28)$; $10 \leqq b > -18$, $2 + b = 28h$, $b = -2$, $h = 0$,
$a' = -4$

$(28, -2, -4)$; $10 \geqq b > 6$, $-2 + b = -4h$, $b = 10$, $h = -2$,
$a' = 28 + 2(-2 - 10) = 4$

$(-4, 10, 4)$ ist eine reducirte Form.

$(956, 366, 140)$; $10 \geqq b > -130$, $366+b=140h$, $b=-86$, $h=2$,
$a'=956-2(366+86)=52$

$(140, -86, 52)$; $10 \geqq b > -42$, $-86+b=52h$, $b=-18$, $h=-2$,
$a'=140+2(-86+18)=4$

$(52, -18, 4)$; $10 \geqq b > 6$, $-18+b=4h$, $b=10$, $h=-2$,
$a'=52+2(-18-10)=-4$

$(4, 10, -4)$ ist eine reducirte Form. $\geqq b > 6$, $10+b=-4h$, $b=10$,
$h=-5$, $a'=4$

$(-4, 10, 4)$.

Hiernach wird die Reihe (4) im vorliegenden Falle:

(5) $(4, 14, 20)$, $(20, 6, -4)$, $(-4, 2, 28)$, $(28, -2, -4)$, $(-4, -10, 4)$, $(4, 18, 52)$, $(52, 86, 140)$, $(140, -366, 956)$, $(956, 366, 140)$;

und die Reihe der zugehörigen Partialquotienten wird:

$h'=1$, $h''=-2$, $h'''=0$, $h^{IV}=3$, $h^{V}=2$, $h^{VI}=2$, $h^{VII}=-2$, $h^{VIII}=0$.

Die Transformationsformeln endlich von $(4, 14, 20)$ in $(956, 366, 140)$ werden auf folgende Art gefunden:

	1	−2	0	3	2	2	−2	0
$\frac{0}{1}$	$\frac{1}{1}$	$\frac{2}{-3}$	$\frac{1}{-1}$	$\frac{1}{0}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{-3}{-5}$	$\frac{-1}{-2}$

und sind $x=-3X-Y$, $y=-5X-2Y$. Hieraus folgt das System $x=\pm 3$, $y=\pm 5$ als eine Lösung der gegebenen Gleichung.

Betrachten wir jetzt das vierte Lösungssystem, welches dem dritten entgegengesetzt ist, so führt dieses auf die Vergleichung der Formen $(4, 14, 20)$ und $(956, -366, 140)$ und wir können aus dem Umstande, dass die Periode der reducirten Formen, welche dem letzteren entspricht, aus den Formen $(-4, 10, 4)$ und $(4, 10, -4)$ sich zusammensetzt und daher mit sich selbst associirt ist (wenn dieser Umstand nicht eintritt, so wird von zwei entgegengesetzten Lösungssystemen immer höchstens eines brauchbar sein), den Schluss ziehen, dass auch das erstere eine Lösung der vorgelegten Gleichung geben müsse.

In der That ist die der Form $(956, -366, 140)$ entsprechende Reihe angrenzender Formen:

$(956, -366, 140)$, $(140, 86, 52)$, $(52, 18, 4)$, $(4, -10, -4)$, $(-4, 10, 4)$

und die Reihe (4) wird im gegenwärtigen Falle:

(4, 14, 20), (20, 6, —4), (—4, 2, 28), (28, —2, 4), (—4, 10, 4)
(4, —18, 52), (52, —86, 140), (140, 366, 956), (956, —366, 140).
Die weitere Rechnung giebt:

	1	—2	0	—2	—2	—2	2	0
$\frac{0}{1}$	$\frac{-1}{1}$	$\frac{2}{-3}$	$\frac{1}{-1}$	$\frac{-4}{5}$	$\frac{7}{-9}$	$\frac{-10}{13}$	$\frac{-27}{35}$	$\frac{10}{-13}$

also ist $x = -27$ und $y = 35$ eine zweite Lösung unserer Gleichung.

Gehen wir zu dem ersten Lösungssysteme fort, so sind die beiden zu vergleichenden Formen (4, 14, 20) und (956, 112, 13); der ersteren entspricht die reducirte Form (—4, 10, 4), der letzteren, wie man sogleich findet, die reducirte Form (13, 5, —7). Bilden wir uns die zu (13, 5, —7) gehörige Periode, so erhalten wir:
(13, 5, —7), (—7, 9, 5), (5, 6, —16), (—16, 10, 1), (1, 10, —16), (—16, 6, 5), (5, 9, —7), (—7, 5, 13), (13, 8, —4), (—4, 8, 13). Darin kommt die Form (4, 14, 20) nicht vor; also ist das erste Lösungssystem unbrauchbar. Da die dem zweiten Lösungssysteme entsprechende Periode der vorstehenden associirt ist und mithin, da letztere mit sich selber associirt ist, geradezu mit ihr zusammenfällt, so ist damit auch das zweite Lösungssystem der Hülfsgleichung als unbrauchbar zu verwerfen. Es resultiren also die 4 Lösungen der vorgegebenen Gleichung:

$$x = +3,\ y = +5;\ x = -3,\ y = -5;\ x = +27,\ y = +35;$$
$$x = -27,\ y = -35.$$

Gehen wir noch einmal auf das dritte Lösungssystem zurück, so führt die Bemerkung, dass die reducirte Form (—4, 10, 4) zu der gegebenen (4, 14, 20) eine zweigliedrige Periode hat, die sich aus den Formen (—4, 10, 4) und (4, 10, —4) zusammensetzt, zu einer unendlichen Menge von Auflösungen. Es ist nämlich offenbar gestattet, in der Reihe (5), die den Uebergang von (4, 14, 20) zu (956, 366, 140) vermittelt, zwischen den Formen (28, —2, —4) und (—4, —10, 4) die genannte Periode so oft, als man irgend will, einzuschieben. Es kommt dies darauf hinaus, in der Reihe der Partialquotienten statt $h^{IV} = 3$, je nachdem die genannte Einschiebung sich 1, 2, 3, 4, ... mal wiederholt, die Grössen —2, 5, 0; —2, 5, —5, 5, 0; —2, 5, —5, 5, —5, 0; —2, 5, —5, 5, —5, 5, —5, 5, 0; ...... zu substituiren.

Führen wir die sich hieran knüpfende Rechnung aus, so erhalten wir:

	1	−2	0	3	2	2	−2	0
$\frac{0}{1}$	$\frac{-1}{1}$	$\frac{2}{3}$	$\frac{1}{-1}$	$\frac{1}{0}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{-3}{-5}$	$\frac{-1}{-2}$

−2	5	0	2	2	−2	0
$\frac{-4}{5}$	$\frac{-21}{26}$	$\frac{4}{-5}$	$\frac{29}{-36}$	$\frac{54}{-67}$	$\frac{-137}{170}$	$\frac{-54}{67}$

−5	5	0	2	2	−2	0
$\frac{109}{135}$	$\frac{566}{-701}$	$\frac{-109}{135}$	$\frac{-784}{971}$	$\frac{-1459}{1807}$	$\frac{3702}{-4585}$	$\frac{1459}{-1807}$

Man hat hiernach folgende drei Lösungen der vorgelegten Gleichung:

$x = \pm 3$ und $y = \pm 5$; $x = \pm 137$ und $y = \mp 170$; $x = \pm 3702$ und $y = \mp 4585$,

welche alle zu derselben Lösung der Bedingungscongruenz $z^2 \equiv 116 \pmod{956}$ gehören und es erhellt, dass noch mehr derartige in unendlicher Anzahl vorhanden sind.

§. 25.

Von den quadratischen Formen mit positiver quadratischer Determinante.

1) Wenn in der Form (A, B, C) die Determinante D von der Form h^2 ist, so kann man der Gleichung $h^2 = B^2 - AC$ die Form geben

$$(1) \quad \frac{h-B}{A} = \frac{-C}{h+B} = \frac{\beta}{\delta},$$

wo β und δ relative Primzahlen gegen einander bezeichnen und das Verhältniss $\frac{\beta}{\delta}$ demzufolge die einfachste Form der beiden gleichen Verhältnisse $\frac{h-B}{A}$ und $\frac{-C}{h+B}$ darstellt. Da β und δ keinen gemeinschaftlichen Factor besitzen, so kann man α und γ so bestimmen, dass sie der Gleichung $\alpha\delta - \beta\gamma = 1$ Genüge leisten. Transformiren wir jetzt die gegebene Form vermöge der Substitutionen $x = \alpha x' + \beta y'$ und $y = \gamma x' + \delta y'$,

so geht die gegebene Form in eine ihr aequivalente Form von der Gestalt $(a, h, 0)$ über. Um dieses zu beweisen hat man, indem man die entstehende Form mit (a, b, c) bezeichnet, darzuthun, dass man $b = h$, $c = 0$ habe. Nun aber ist zu Folge der allgemeinen Transformationsformeln $b = A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta$, $c = A\beta^2 + 2B\beta\delta + C\delta^2$, also, wenn man hier für A und C ihre aus (1) gezogenen Werthe $A = (h - B)\frac{\delta}{\beta}$ und $C = -(h + B)\frac{\beta}{\delta}$ einsetzt, $b = (h - B)\alpha\delta + B(\alpha\delta + \beta\gamma) - (h + B)\beta\gamma = h(\alpha\delta - \beta\gamma) = h$, $c = (h - B)\beta\delta + 2B\beta\delta - (h + B)\beta\delta = 0$. Wenn nun die Zahl a, die aus dieser Transformation fliesst, zwischen den Grenzen 0 und $2h - 1$ liegt oder einer dieser Grenzen gleich ist, so heisst die Form $(a, h, 0)$ die reducirte Form zu der gegebenen. Sollte sie dieser Bedingung noch nicht sogleich Genüge leisten, so erhält man die reducirte Form, wenn man an Stelle von a den kleinsten positiven Rest a' dieser Zahl nach dem Modul $2h$ setzt, so dass man $a \equiv a' \pmod{2h}$ oder $\frac{a - a'}{2h}$ = Num. integ. hat. Es ist nämlich die Form $(a, h, 0)$ der Form $(a', h, 0)$ aequivalent. Diese Aequivalenz findet statt, weil einmal die beiden Determinanten gleich sind und dann eine Transformation der ersten Form in die zweite existirt, nämlich (wenn wir die Unbestimmten respective mit x', y' und x'', y'' bezeichnen) $x' = x''$ und $y' = \frac{a - a'}{2h}x'' + y''$.

Von den reducirten Formen gelten folgende Sätze und Erklärungen:

Eine reducirte Form zu einer gegebenen Form mit positiver quadratischer Determinante h^2 ist eine solche Form, die der gegebenen im eigentlichen Sinne aequivalent ist, deren mittelster Coefficient gleich h, deren letzter Coefficient gleich 0 und deren erster Coefficient zwischen den Zahlen 0 und $2h - 1$ liegt oder einer dieser beiden Grenzen selbst gleich ist.

Zwei reducirte Formen können nur dann eigentlich aequivalente sein, wenn sie identische Formen sind; es existiren daher zu einer gegebenen Determinante h^2 $2h$ von einander verschiedene reducirte Formen, welche ebensovielen Klassen von Formen entsprechen.

Nehmen wir an, $(a, h, 0)$ und $(a', h, 0)$ wären zwei reducirte aequivalente Formen und die erste ginge in die zweite über durch die Substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, so hätte man die 4 Gleichungen:

$$(2)\quad a\alpha^2 + 2h\alpha\gamma = a'; \qquad (3)\quad a\alpha\beta + h(\alpha\delta + \beta\gamma) = h;$$

$$(4)\quad a\beta^2 + 2h\beta\delta = 0; \qquad (5)\quad \alpha\delta - \beta\gamma = 1.$$

Eliminirt man aus der dritten und vierten Gleichung a, so folgt $h(-\alpha\beta\delta + \beta^2\gamma) = 0$, woher, da die Grösse in der Klammer sich auf $-\beta(\alpha\delta - \beta\gamma) = -\beta$ reducirt, nothwendig $\beta = 0$ sein muss. Demgemäss folgt aus (5) $\alpha\delta = 1$, $\alpha = \pm 1$, $\delta = \pm 1$. Setzt man jetzt in (2) für α seinen Werth, so bekommen wir $a \pm 2h\gamma = a'$ oder $a' \equiv a \ (mod\ 2h)$. Da diese Congruenz zwischen den Grenzen 0 und $2h$ nur eine Lösung gestattet, so hat man $a' = a$, d. h. die beiden Formen sind identisch.

Betrachten wir, um ein Beispiel zu haben, die auf die Determinante 25 bezüglichen reducirten Formen, so zerfallen diese in 10 Klassen, die den Formen

$$(0, 5, 0), (1, 5, 0), (2, 5, 0), (5, 5, 0), (8, 5, 0), (9, 5, 0);$$
$$(3, 5, 0), (7, 5, 0); (4, 5, 0), (6, 5, 0)$$

respective entsprechen. Von diesen Formen sind die 6 ersten unter einander uneigentlich aequivalent, ferner die 7te und 8te, endlich die 9te und 10te.

Wenn zwei beliebig aequivalente Formen gegeben sind, eine Transformation der einen in die andere zu finden.

Seien die beiden gegebenen Formen $F = (A, B, C)$ mit den Unbestimmten X, Y und $f = (a, b, c)$ mit den Unbestimmten x, y; die reducirte Form zu beiden möge $(a', h, 0)$ sein mit den Unbestimmten x' y'. Indem wir die allgemeinen Principien über Transformationen (cf. §. 22. unter 2.) auf die beiden anwenden, welche zur Reduction irgend einer Form nothwendig sind, erhellt unmittelbar, dass die Substitutionen, vermöge welcher F und f in die Form $(a', h, 0)$ übergehen, folgende sind:

$$(6)\quad X = \alpha_{,} x' + \beta_{,} y', \quad Y = \gamma_{,} x' + \delta_{,} y',$$

$$(7)\quad x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'.$$

Vermöge (7), unter Zuziehung der Gleichung $\alpha'\delta' - \beta'\gamma' = 1$, findet man

$$x' = \delta' x - \beta y', \quad y' = -\gamma' x + \alpha' y$$

und diese Werthe für x' und y' in (6) einsetzend erhalten wir die gesuchten Transformationsformeln, vermöge welcher f in F übergeht, nämlich:

(8) $X = (\alpha,\ \delta' - \beta,\ \gamma')x + (\beta,\ \alpha' - \alpha,\ \beta')y,\quad Y = (\gamma,\ \delta' - \delta,\ \gamma')x + (\delta,\ \alpha' - \gamma,\ \beta')y.$

2) Die entwickelten Principien sind ausreichend zur Lösung des fundamentalen Theoremes, die Gleichung $Ax^2 + 2Bxy + Cy^2 = M$ in ganzen Zahlen für x, y aufzulösen. Die Art ihrer Anwendung bietet nichts Neues dar, was aus dem Vorigen nicht von selbst erhellte; wir ziehen es daher vor eine andere Lösung desselben Problemes zu geben, welche auf Principien beruht, die der speciellen Natur des betrachteten Falles angepasst sind.

Nehmen wir zu dem Zwecke die Gleichungen (1) wieder auf, welche sich auf die Gleichung

$$(9)\quad Ax^2 + 2Bxy + Cy^2 = M$$

beziehen und folgern aus ihnen, dass β nothwendig in $h - B$ und $-C$ ohne Rest aufgeht und ebenso δ in A und $h + B$: dann kann man, indem p und q ganze Zahlen bezeichnen, setzen $\frac{h-B}{\beta} = \frac{A}{\delta} = p$ und $\frac{h+B}{\delta} = \frac{-C}{\beta} = q$ und es lässt sich die Identität der Ausdrücke $(\delta x - \beta y)(px + qy)$ und $Ax^2 + 2Bxy + Cy^2$ nachweisen. Demgemäss kann man die Gleichung (9) ersetzen durch die folgende:

$$(10)\quad (\delta x - \beta y)(px + qy) = M.$$

Man suche sich jetzt alle möglichen positiven oder negativen Theiler von M, und löse, indem m allgemein irgend einen dieser Theiler bezeichnet, die beiden Gleichungen

$$(11)\quad \delta x - \beta y = m, \qquad (12)\quad px + qy = \frac{M}{m}$$

auf, die in ihrem Zusammenbestehen mit (9) identisch sind. Auf diese Weise resultirt

$$(13)\quad x = \frac{M\beta + qm^2}{m(\beta p + \delta q)},\quad y = \frac{M\delta - pm^2}{m(\beta p + \delta q)}.$$

Diese Gleichungen geben immer bestimmte und endliche Werthe für x und y, weil der Ausdruck $\beta p + \delta q = (h - B) + (h + B) = 2h$ und ebenso m eine bestimmte endliche Grösse ist.

So z. B. ergeben sich für die Gleichung $3x^2 + 4xy + 7y^2 = 12$ nur 2 Auflösungen, nämlich $x = \pm 2$, $y = 0$.

Die vorgetragene Auflösung setzt stillschweigend voraus, dass die Zerlegung von M in endliche Factoren möglich ist, d. h. dass M von 0 verschieden sei. Wenn $M=0$ und mithin die Gleichung

$$Ax^2+2Bxy+Cy^2=0$$

oder die mit ihr identische

$$(\delta x+\beta y)(px+qy)=0$$

aufzulösen ist, so sind zwei von einander verschiedene Lösungen möglich, indem man sowohl $\delta x-\beta y=0$, wie $px+qy=0$ setzen kann. Wir bekommen dadurch, indem z eine beliebige ganze positive oder negative Zahl und m den grössten gemeinschaftlichen Divisor der Zahlen p und q bezeichnet, die beiden Lösungssysteme:

$$x=\beta z,\ y=\delta z \text{ und } x=\frac{q}{m}z,\ \ y=-\frac{p}{m}z.$$

3) Wenn die Determinante D der Gleichung $Ax^2+2Bxy+Cy^2=M$ der Null gleich ist, so hat man $B^2-AC=0$ und die Gleichung geht durch Multiplication mit A über in $(Ax+By)^2=AM$. Damit sie also möglich sei, ist nothwendig, dass AM ein vollständiges Quadrat und also von der Form K^2 sei: dies vorausgesetzt hat man jede der unbestimmten Gleichungen $Ax+By=K$ und $Ax+By=-K$ in ganzen Zahlen für x und y aufzulösen: die gegebene Gleichung ist also zurückführbar auf 2 Congruenzen des ersten Grades und damit dieselben möglich seien, ist nothwendig und hinreichend, dass der grösste gemeinschaftliche Theiler zwischen A und B auch die Zahl K theile.

§. 26.

Von den verschiedenen unter einander ähnlichen Transformationen einer gegebenen Form in eine andere gegebene Form.

Das allgemeine Problem, die Repräsentationen einer Zahl M durch eine Form $F=(A,\ B,\ C)$ von gegebener Zusammensetzung zu finden, haben wir in allen Fällen auf das Problem der Transformation der Form F in eine andere zurückgeführt, welche sich aus einer gewissen Bedingungsgleichung in bekannter Weise ergiebt, und jeder eigentlichen Transfor-

mation entspricht eine specielle Repräsentation (oder in gewissen Fällen eine unendliche Menge von Repräsentationen, die jedoch mit dieser speciellen einen innigen und genauen Zusammenhang haben; man vergleiche hierüber das, was am Schlusse des §. 24 gesagt ist). Zugleich haben wir gezeigt, wie man immer wenigstens eine specielle Transformation sich bestimmen könne. Hiermit, wenn wir anders alle nur möglichen von einander verschiedenen Lösungen finden wollen, sind wir genöthigt, uns zuvor mit dem folgenden fundamentalen Probleme zu beschäftigen:

Wenn uns zwei Formen $F = AX^2+2BXY+CY^2$ und $f = ax^2+2bxy+cy^2$ und irgend eine specielle Transformation der ersten in die letzte gegeben sind, aus dieser einen alle nur möglichen von einander verschiedenen ähnliche Transformationen herzuleiten.

Die bekannte Transformation möge sich vollführen durch die Substitutionen $X = \alpha x+\beta y$ und $Y = \gamma x+\delta y$; wir wollen annehmen, irgend eine davon verschiedene und ihr ähnliche Transformation sei $X = \alpha' x+\beta' y$ und $Y = \gamma' x+\delta' y$. Sei ferner die Determinante der beiden Formen F und f respective D und d, ferner $\alpha\delta-\beta\gamma = e$, $\alpha'\delta'-\beta'\gamma' = e'$, so sind e und e' Grössen von gleichem Vorzeichen, weil beide Transformationen ähnlich sind (cf. §. 22, 2.) und man hat $d = De^2$ und $d = De'^2$, also $e^2 = e'^2$ und daher $e = e'$, d. h. es ist

$$e = e' = \alpha\delta-\beta\gamma = \alpha'\delta'-\beta'\gamma'.$$

Es bestehen ferner zu Folge der Natur der Transformationen die Gleichungen:

$$(1)\quad A\alpha^2+2B\alpha\gamma+C\gamma^2 = a,\qquad (2)\quad A\alpha'^2+2B\alpha'\gamma'+C\gamma'^2 = a$$

$$(3)\quad A\alpha\beta+B(\alpha\delta+\beta\gamma)+C\gamma\delta = b,\qquad (4)\quad A\alpha'\beta'+B(\alpha'\delta'+\beta'\gamma')+C\gamma'\delta' = b$$

$$(5)\quad A\beta^2+2B\beta\delta+C\delta^2 = c,\qquad (6)\quad A\beta'^2+2B\beta'\delta'+C\delta'^2 = c.$$

Setzen wir der Abkürzung halber:

$$A\alpha\alpha'+B(\alpha\gamma'+\gamma\alpha')+C\gamma\gamma' = A'$$

$$A(\alpha\beta'+\beta\alpha')+B(\alpha\delta'+\beta\gamma'+\gamma\beta'+\delta\alpha')+C(\gamma\delta'+\delta\gamma') = 2B'$$

$$A\beta\beta'+B(\beta\delta'+\delta\beta')+C\delta\delta' = C';$$

alsdann erhalten wir aus dem vorstehenden Systeme von Gleichungen die folgenden:

$$(7)\quad A'^2-D(\alpha\gamma'-\gamma\alpha')^2 = a^2$$

$$(8)\quad 2A'B'-D(\alpha\gamma'-\gamma\alpha')(\alpha\delta'+\beta\gamma'-\gamma\beta'-\delta\alpha') = 2ab$$

$$(9) \quad 4B'^2 - (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4b^2$$

$$(10) \quad A'C' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac$$

$$(11) \quad 2B'C' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc$$

$$(12) \quad C'^2 - D(\beta\delta' - \delta\beta')^2 = c^2.$$

Die Gleichung (7) folgt aus (1).(2), die Gleichung (8) aus (1).(4)+(2).(3), die Gleichung (9) aus (1).(6)+(2).(5)+2.(3).(4); die Gleichung (10) ergiebt sich, indem man (3) mit (4) multiplicirt und davon die Gleichung $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = b^2 - ac$ abzieht; die Gleichung (11) ist (3).(6)+(4).(5) und die Gleichung (12) ist (5).(6).

Nehmen wir jetzt an, der grösste gemeinschaftliche Divisor der Zahlen a, $2b$, c wäre m: dann kann man immer die Zahlen g, h, k so bestimmen, dass sie der Gleichung

$$ag + 2bh + ck = m$$

Genüge leisten und zwar auf unendlich vielfache Weise.

Setzen wir, um dieses darzuthun, für den Augenblick den grössten gemeinschaftlichen Divisor zwischen a und $2b$ gleich l, so ist der grösste gemeinschaftliche Divisor zwischen l und c die Zahl m: demzufolge sind $\frac{a}{l}$ und $\frac{2b}{l}$, $\frac{l}{m}$ und $\frac{c}{m}$ respective relative Primzahlen und die beiden unbestimmten Gleichungen $\frac{a}{l}x + \frac{2b}{l}y = 1$ und $\frac{l}{m}u + \frac{c}{m}z = 1$ immer in ganzen Zahlen für x und y, u und z auflösbar. Nun sind dieselben identisch mit den Gleichungen $ax + 2by = l$, $lu + cz = m$, woraus durch Einsetzung der ersten in die letzte $axu + 2byu + cz = m$ folgt, also hat man $g = xu$, $h = yu$, $k = z$.

Dieses vorausgesetzt multiplicire man die Gleichungen (7), (8), (9), (10), (11), (12) der Reihe nach durch die Zahlen g^2, $2gh$, h^2, $2gk$, $2hk$, k^2 und addire die Producte zusammen: es resultirt schliesslich

$$(A'g + 2B'h + C'k)^2 - D\Big\{g(\alpha\gamma' - \gamma\alpha') + h(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta') + k(\beta\delta' - \delta\beta')\Big\}^2 = m^2$$

oder, wenn man, um abzukürzen,

$$(13) \quad A'g + 2B'h + C'k = T$$

$$(14) \quad g(\alpha\gamma' - \gamma\alpha') + h(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta') + k(\beta\delta' - \delta\beta') = U$$

setzt, man kommt zurück auf die einfache Gleichung zwischen den beiden Unbestimmten T und U:

$$T^2 - DU^2 = m^2.$$

Hiermit haben wir das bemerkenswerthe Theorem gewonnen: Aus je zwei unter einander ähnlichen Transformationen der Form F in die Form f kann man eine Lösung der unbestimmten Gleichung $t^2 - Du^2 = m^2$ in ganzen Zahlen für t und u sich herleiten, nämlich $t = T$ und $u = U$.

Weiter unten werden wir bequemere Ausdrücke zur Berechnung der Grössen T und U entwickeln, aus denen namentlich auch hervorgeht, dass der Werth dieser Grössen von der speciellen Beschaffenheit der Zahlen g, h, k vollkommen unabhängig sich bestimmt. — Die beiden Transformationen, welche unter der Voraussetzung, dass sie ähnlich, d. h beide entweder eigentliche oder uneigentliche sind, eine Lösung der Gleichung $t^2 - Du^2 = m^2$ liefern, sind vollkommen willkürlich und können daher auch identisch sein. In diesem Falle liefern sie die specielle Lösung $u = 0$ und $t = \pm m$, welche bei der ersten Betrachtung der Gleichung unmittelbar erhellt.

Der vorstehende Satz stellt ein Verhältniss der Abhängigkeit fest zwischen zwei Transformationen der Form F in die Form f und einer speciellen Lösung unserer Gleichung; da nun von diesen zwei Transformationen nur eine bekannt, die andere gesucht, so liegt es nahe die Untersuchung umzukehren und zu sehen, in welchem Abhängigkeitsverhältnisse diese unbekannte Transformation zu der bekannten Transformation und der zugehörigen speciellen Lösung unserer Gleichung zwischen t und u stehe.

Zu dem Zwecke entwickeln wir folgende Gleichungen:

$$(15)\quad (\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma')A' = a(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha'),$$

$$(16)\quad (\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma')B' = 2b(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha'),$$

$$(17)\quad (\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma')C' = c(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha').$$

Die Gleichung (15) entsteht aus $(1).(\delta\alpha' - \beta\gamma') + (2).(\alpha\delta' - \gamma\beta') + (3).(\alpha\gamma' - \gamma\alpha') + (4).(\gamma\alpha' - \alpha\gamma')$, die Gleichung (16) aus $((1) - (2)).(\delta\beta' - \beta\delta') + ((3) + (4)).(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha') + ((5) - (6))(\alpha\gamma' - \gamma\alpha')$, die Gleichung (17) endlich aus $((3) - (4))(\delta\beta' - \beta\delta') + (5).(\alpha\delta' - \gamma\beta') + (6).(\delta\alpha' - \beta\gamma')$.

Aus den Gleichungen (15), (16), (17) zieht man unter Benutzung der Relation $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma'$:

$$A' = \frac{a(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')}{2(\alpha\delta - \beta\gamma)},\quad 2B' = \frac{2b(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')}{2(\alpha\delta - \beta\gamma)},$$

$$C' = \frac{c(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')}{2(\alpha\delta - \beta\gamma)}$$

und indem wir diese Werthe für A', $2B'$, C' in (13) einsetzen, erhalten wir

$$(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(ag + 2bh + ck) = 2(\alpha\delta - \beta\gamma)T,$$

woher, wenn man für $ag + 2bh + ck$ seinen Werth m setzt,

$$(18)\quad 2(\alpha\delta - \beta\gamma)T = m(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha');$$

diese letzte Gleichung bietet ein zur Berechnung von T bequemes Mittel dar und zeigt dessen vollständige Unabhängigkeit von den speciellen Zahlenwerthen der Unbestimmten g, h, k.

Indem wir die Gleichung (18) durch jede der Gleichungen (15), (16), (17) dividiren, sind die Resultate

$$mA' = Ta,\quad 2mB' = 2Tb,\quad mC' = Tc$$

und wir können hieraus die Werthe von A', $2B'$, C' ziehen; setzen wir dieselben in die Gleichungen (7), (8), ... (12) ein, substituiren für T^2 seinen Werth $m^2 + DU^2$, so erhalten wir:

$$\begin{array}{ll}
(a) & (\alpha\gamma' - \gamma\alpha')^2 m^2 = a^2U^2 \\
(ab) & (\alpha\gamma' - \gamma\alpha')(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')m^2 = 2abU^2 \\
(b) & (\alpha\delta' - \alpha'\delta' + \beta\gamma' - \gamma\beta')^2 m^2 = 4b^2U^2 \\
(ac) & (\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')m^2 = acU^2 \\
(bc) & (\beta\delta' - \delta\beta')(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')m^2 = 2bcU^2 \\
(c) & (\beta\delta' - \delta\beta')^2 m^2 = c^2U^2.
\end{array}$$

Aus diesem Gleichungssysteme folgt, indem man sich der Reihe nach die Combinationen

$$g.(a) + h.(ab) + k.(ac);\quad g.(ab) + h.(b) + k.(bc);\quad g.(ac) + h.(bc) + k.(c)$$

bildet, das folgende neue

$$(\alpha\gamma' - \gamma\alpha').Um^2 = maU^2,$$

$$(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')Um^2 = 2mbU^2$$

$$(\beta\delta' - \delta\beta').Um^2 = mcU^2$$

und hieraus, indem man mU auf beiden Seiten dividirt,

$$(19)\quad aU = m(\alpha\gamma' - \gamma\alpha')$$

$$(20)\quad 2bU = m(\alpha\delta' - \delta\alpha' + \beta\gamma' - \gamma\beta')$$

$$(21)\quad cU = m(\beta\delta' - \delta\beta').$$

Jede dieser 3 Gleichungen ist gleich geeignet zur Berechnung von U und zeigt, in Uebereinstimmung mit der obigen Aussage, die Unabhängigkeit dieser Grösse von der speciellen Natur der g, h, k.

Es ergeben sich ferner durch die Bildung der Gleichungen (18) + (20) und (18) — (20):

$$(22)\quad (\alpha\delta-\beta\gamma)T+bU=m(\alpha\delta'-\gamma\beta')$$

$$(23)\quad (\alpha\delta-\beta\gamma)T-bU=m(\delta\alpha'-\beta\gamma').$$

Die Gleichungen (19), (21), (22) und (23) bilden ein System von 4 Gleichungen, in denen ausser den 4 unbekannten Grössen α', β', γ', δ' lauter entweder unmittelbar bekannte oder doch leicht bestimmbare Grössen vorkommen; wir sind daher im Stande aus ihnen in bekannter Weise die Werthe der 4 Grössen α', β', γ', δ' herzuleiten und erhalten, wenn wir noch für a, b, c ihre Werthe aus den Gleichungen (1), (3), (5) substituiren:

$$\alpha'=\frac{1}{m}\left\{\alpha T-(B\alpha+C\gamma)U\right\},$$

$$\beta'=\frac{1}{m}\left\{\beta T-(B\beta+C\delta)U\right\},$$

$$\gamma'=\frac{1}{m}\left\{\gamma T+(A\alpha+B\gamma)U\right\},$$

$$\delta'=\frac{1}{m}\left\{\delta T+(A\beta+B\delta)U\right\}.$$

Die gesuchte Transformation steht demzufolge unter der Form

$$(24)\quad \left\{\begin{aligned} X&=\frac{1}{m}\left\{\alpha T-(B\alpha+C\gamma)U\right\}x+\frac{1}{m}\left\{\beta T-(B\beta+C\delta)U\right\}y,\\ Y&=\frac{1}{m}\left\{\gamma T+(A\alpha+B\gamma)U\right\}x+\frac{1}{m}\left\{\delta T+(A\beta+B\delta)U\right\}y.\end{aligned}\right.$$

Es ist leicht, dadurch, dass man die Werthe von α', β', γ', δ' in die Formeln (2), (4), (6) einsetzt und die Gleichung $T-DU^2=m^2$ anwendet, den Beweis zu führen, dass vermöge ihrer die Form F in f übergeht; eben so leicht erhellt die Gleichung $\alpha\delta-\beta\gamma=\alpha'\delta'-\beta'\gamma'$, d. h. die Bedingung für ihre Aehnlichkeit mit der gegebenen.

Aus unserer Analyse folgt, dass keine Transformation der Form F in f, welche der gegebenen ähnlich ist, existiren könne, die nicht unter den Formeln (24) enthalten sei und demzufolge irgend einer speciellen Lösung der Gleichung $t^2-Du^2=m^2$ entspreche. Aber es ist darum nicht

unbedingt nothwendig, dass jede Lösung dieser Gleichung auch eine mit der gegebenen Transformation ähnliche liefern müsse; denn es kann offenbar vorkommen, dass für gewisse specielle Zahlenwerthe von t und u die Coefficienten von x und y in den Formeln (21) entweder alle oder zum Theil gebrochene Zahlen werden, was mit dem früher aufgestellten Begriffe der Transformation nur durch ganzzahlige Substitutionen bewirkt zu werden im Widerspruch stehen würde. Es lässt sich aber der Nachweis führen, dass dergleichen niemals statthaben kann, wenn die beiden Determinanten d und D einander gleich sind, d. h. wenn die beiden Formen F und f einander aequivalent sind, und dies ist zugleich der einzige Fall, dessen wir für unsere Zwecke bedürfen. Wir haben alsdann das Theorem:

Wenn die Formen F und f einander aequivalent sind, so liefert jedes Lösungssytem der Gleichung $t^2-Du^2=m^2$ zu irgend einer gegebenen Transformation eine zweite derselben ähnliche.

Wir haben m als den grössten gemeinschaftlichen Divisor zwischen den Zahlen a, $2b$, c angenommen; da nun die Formen (A, B, C) und (a, b, c) aequivalente sind, so muss, gemäss dem Theorem 2) in §. 22, m auch der grösste gemeinschaftliche Divisor zwischen den Zahlen A, $2B$, C sein. Nun ist $4T^2-4DU^2=4m^2$ und da $4DU^2$ (wegen $4D=(2B)^2-AC$) und $4m^2$ durch m^2 theilbar sind, so muss auch $4T^2$ durch m^2 theilbar sein, also $2T$ durch m. Hiernach sind die Ausdrücke $\frac{2}{m}(T+BU)$ und $\frac{2}{m}(T-BU)$ ganze Zahlen. Nun ist die Differenz $\frac{4BU}{m}$ dieser beiden Zahlen immer gerade, also sind sie entweder beide zu gleicher Zeit gerade oder beide ungerade. Nun können sie nicht zu gleicher Zeit ungerade sein, weil ihr Product $\frac{4}{m^2}(T^2-B^2U^2)$ eine gerade Zahl ist — es folgt nämlich aus $T^2-DU^2=m^2$ der Ausdruck $T^2-B^2U^2+ACU^2$ als ein Vielfaches von m^2 und da ACU^2 für sich allein auch schon ein solches Vielfaches ist, so ist es auch $T^2-B^2U^2$, mithin $\frac{1}{m^2}(T^2-B^2U^2)$ eine ganze Zahl —; also folgt, dass sie beide gleichzeitig gerade Zahlen sind und die Ausdrücke $\frac{1}{m}(T-BU)$ und $\frac{1}{m}(T+BU)$ darum ganze Zahlen. Dies

sind aber, da A und C ausserdem für sich allein durch m theilbar, die zureichenden Bedingungen dafür, dass die Substitutionen (24) nur ganzzahlige Coefficienten enthalten.

Beispiel. Die Form (1, 0, 2) geht durch die eigentliche Transformation $x = 2x' + 7y'$, $y = x' + 5y'$ über in die Form (6, 24, 99). Da wir $D = -2$ haben und 3 der grösste gemeinschaftliche Divisor zwischen 6, 24, 99 ist, so nimmt die Gleichung $t^2 - Du^2 = m^2$ die specielle Gestalt $t^2 + 2u^2 = 9$ an, der, wie man sich leicht überzeugt, folgende 6 (und ausserdem keine anderen) Systeme von Werthen der t, u genügen:

$$t = 3,\ u = 0;\ t = -3,\ u = 0;\ t = 1,\ u = 2;\ t = -1,\ u = 2;$$
$$t = 1,\ u = -2;\ t = -1,\ u = -2.$$

Die dritte und sechste unter diesen Lösungssystemen geben Substitutionen mit gebrochenen Coefficienten und sind daher unbrauchbar; die 4 anderen geben vermöge der Formeln (24) folgende Substitutionen:

$$\begin{aligned} x &= 2x' + 7y', & y &= x' + 5y' \\ x &= -2x' + 7y', & y &= -x' + 5y' \\ x &= 2x' + 9y', & y &= x' + 3y' \\ x &= -2x' + 9y', & y &= -x' + 3y'. \end{aligned}$$

Die erste unter diesen Transformationen fällt mit der gegebenen zusammen.

Durch das Problem der Transformation werden wir mithin weiter zu dem Probleme hingetrieben, die Gleichung $t^2 - Du^2 = m^2$ in ganzen Zahlen für t und u aufzulösen oder mit anderen Worten alle nur möglichen Repräsentationen der Zahl m^2 durch die Form $t^2 - Du^2$ zu finden. Dieses letztere Problem ist nur ein specieller Fall des allgemeinen, von welchem wir ausgegangen sind und da wir nur nöthig haben es unter der Annahme aufzulösen, dass die Zahlen D und m durch eine bestimmte Form (A, B, C) gegeben sind, soll es in dem folgenden Paragraphen in dieser seiner Verknüpfung mit dem allgemeinen Probleme betrachtet werden.

§. 27.

Theorie der Gleichung $t^2-Du^2=m^2$ und Anwendung derselben auf das Problem, die allgemeine Gleichung $Ax^2+Bxy+Cy^2=M$ in ganzen Zahlen für x und y aufzulösen.

Die Natur der Gleichung $t^2-Du^2=m^2$ macht die Unterscheidung zweier Hauptfälle nöthig, welche durch das Vorzeichen von D ihre Bestimmung erhalten. Nämlich die Determinante D kann entweder positiv oder negativ sein und wir haben daher, wenn wir unter D eine absolute oder auch eine wesentlich positive Zahl verstehen, die beiden Formen $t^2+Du^2=m^2$ und $t^2-Du^2=m^2$ in abgesonderter Weise zu betrachten. Zuvor schicken wir aber noch eine allgemeine auf beide Fälle gleichmässig bezügliche Bemerkung voraus.

Die Gleichung $t^2\pm Du^2=m^2$ steht, wie wir gesehen haben, mit den beiden zusammengehörigen Formen $F=Ax^2+2Bxy+Cy^2$ und $f=M\xi^2+2z\xi\eta+s\eta^2$ in einem innigen Zusammenhange; nämlich m bezeichnet den grössten gemeinschaftlichen Divisor sowohl der Coefficienten A, $2B$, C, wie auch der Coefficienten M, $2z$, s und ausserdem wissen wir, dass je zwei Transformationen von (A, B, C) in (M, z, s) eine Lösung unserer Gleichung bestimmen, und umgekehrt, dass durch eine Transformation und eine solche Lösung immer eine zweite Transformation bestimmt wird. Da nun die beiden Transformationen, welche eine Lösung bestimmen, auch zusammenfallen können und, indem sie zusammenfallen, die particuläre Lösung $u=0$ und $t=+u$ hervorbringen, ergiebt sich, dass soviel eigentliche Transformationen von F und f existiren, als von einander verschiedene Lösungen der Gleichung $t^2\pm Du^2=m^2$. Eine specielle Transformation von (A, B, C) in (M, z, s) kann nun immer in der bekannten Weise vermöge einer Reihe von angrenzenden Formen gefunden werden. Sei diese Transformation dargestellt durch $x=\alpha\xi+\beta\eta$, $y=\gamma\xi+\delta\eta$, so gehört zu derselben die Lösung $u=0$, $t=+m$, und zu der entgegengesetzten (ebenfalls eigentlichen) Transformation $x=-\alpha\xi-\beta\eta$, $y=-\gamma\xi-\delta\eta$ gehört die entgegengesetzte Lösung $u=0$, $t=-m$. Indem wir uns das Problem, die

Gleichung $t^2 \pm Du^2 = m^2$ aufzulösen, stellen, wird es uns daher wesentlich nur um solche Lösungssysteme zu thun sein, welche von den beiden genannten verschieden sind. Ein jedes darunter wird als zu einer speciellen und vermöge der Formeln (24) im vorigen Paragraphen bestimmbaren Transformation gehörig betrachtet werden können. Zu je zwei entgegengesetzten Lösungssystemen gehören auch immer je zwei einander entgegengesetzte Transformationen.

1) Auflösung der Gleichung $t^2 + Du^2 = m^2$. Die Zahl der Lösungen ist in diesem Falle eine beschränkte und es lassen sich folgende Fälle unterscheiden:

a) $\frac{4D}{m^2} > 4$ oder $D > m^2$. In diesem Falle existiren ersichtlich nicht mehr als zwei von einander verschiedene Lösungssysteme, nämlich $u = 0$ und $t = \pm m$. Mithin existiren auch nicht mehr als zwei und zwar einander entgegengesetzte Transformationen von F in f, nämlich $x = \alpha\xi + \beta\eta$ und $y = \gamma\xi + \delta\eta$, $x = -\alpha\xi - \beta\eta$ und $y = -\gamma\xi - \delta\eta$. Dem entsprechend hat die Gleichung $Ax^2 + 2Bxy + Cy^2 = M$ nicht mehr als zwei von einander verschiedene und zwar einander gerade ertgegengesetzte Lösungen, nämlich $x = +\alpha$ und $y = +\gamma$, $x = -\alpha$ und $y = -\gamma$.

b) $\frac{4D}{m^2} = 4$ oder $D = m^2$. In diesem Falle existiren 4 und nicht mehr von einander verschiedene Lösungssysteme: $u = 0$ und $t = +m$, $u = 0$ und $t = -m$, $u = 1$ und $t = 0$, $u = -1$ und $t = 0$; dieselben geben in die Formeln (24) eingesetzt nach einander folgende 4 verschiedene (eigentliche) Transformationen:

$$x = \alpha\xi + \beta\eta \text{ und } y = \gamma\xi + \delta\eta, \quad x = -\alpha\xi - \beta\eta \text{ und } y = -\gamma\xi - \delta\eta,$$

$$x = -\frac{B\alpha + C\gamma}{m}\xi - \frac{B\beta + C\delta}{m}\eta \text{ und } y = \frac{A\alpha + B\gamma}{m}\xi + \frac{A\beta + C\delta}{m}\eta$$

$$x = +\frac{B\alpha + C\gamma}{m}\xi + \frac{B\beta + C\delta}{m}\eta \text{ und } y = -\frac{A\alpha + B\gamma}{m}\xi - \frac{A\beta + C\delta}{m}\eta.$$

Dem entsprechend hat die Gleichung $Ax^2 + 2Bxy + Cy^2 = M$ nicht mehr als 4 von einander verschiedene Lösungssysteme, die sich in Gruppen zu je zwei einander entgegengesetzten ordnen lassen, nämlich:

$$x = \alpha \text{ und } y = \gamma; \quad x = -\alpha \text{ und } y = -\gamma;$$

$$x = -\frac{B\alpha + C\gamma}{m} \text{ und } y = \frac{A\alpha + B\gamma}{m}; \quad x = \frac{B\alpha + C\gamma}{m} \text{ und } y = -\frac{A\alpha + B\gamma}{m}.$$

c) $\frac{4D}{m^2}=3$ oder $4D=3m^2$. In diesem Falle wird m mit Nothwendigkeit eine gerade Zahl sein und die Gleichung $t^2+Du^2=m^2$ hat 6 verschiedene Lösungssysteme, nämlich: $u=0$, $t=m$; $u=0$, $t=-m$; $u=1$, $t=\frac{1}{2}m$; $u=-1$, $t=-\frac{1}{2}m$; $u=-1$, $t=\frac{1}{2}m$; $u=1$, $t=-\frac{1}{2}m$ und man hat folgende 6 Transformationen, die sich paarweise zu je zwei, die einander entgegengesetzt sind, wie folgt, anordnen lassen:

$$x=\pm\alpha\xi\pm\beta\eta,\quad y=\pm\gamma x'\pm\delta\eta;$$

$$x=\pm\left(\frac{\alpha}{2}-\frac{B\alpha+C\gamma}{m}\right)\xi\pm\left(\frac{\beta}{2}-\frac{B\beta+C\delta}{m}\right)\eta.$$

$$y=\pm\left(\frac{\gamma}{2}+\frac{A\alpha+B\gamma}{m}\right)\eta\pm\left(\frac{\delta}{2}+\frac{B\beta+C\delta}{m}\right)\eta;$$

$$x=\pm\left(\frac{\alpha}{2}+\frac{B\alpha+C\gamma}{m}\right)\xi\pm\left(\frac{\beta}{2}+\frac{B\beta+C\delta}{m}\right)\eta,$$

$$y=\pm\left(\frac{\gamma}{2}-\frac{A\alpha+B\gamma}{m}\right)\xi\pm\left(\frac{\delta}{2}-\frac{B\beta+C\delta}{m}\right)\eta.$$

Wir erhalten dadurch 6 verschiedene Lösungen der Gleichung $Ax^2+2Bxy+Cy^2=M$, ausser denen sonst weiter keine existiren, nämlich:

$$x=\alpha,\ y=\gamma;\ x=-\alpha,\ y=-\gamma;$$

$$x=\frac{\alpha}{2}-\frac{B\alpha+C\gamma}{m},\ y=\frac{\gamma}{2}+\frac{A\alpha+B\gamma}{m};\ x=-\frac{\alpha}{2}+\frac{B\alpha+C\gamma}{m},$$

$$y=-\frac{\gamma}{2}-\frac{A\alpha+B\gamma}{m};$$

$$x=\frac{\alpha}{2}+\frac{B\alpha+C\gamma}{m},\ y=\frac{\gamma}{2}-\frac{A\alpha+B\gamma}{m};\ x=-\frac{\alpha}{2}-\frac{B\alpha+C\gamma}{m},$$

$$y=-\frac{\gamma}{2}+\frac{A\alpha+B\gamma}{m}.$$

d) Es könnte scheinen, dass zu den bezeichneten Fällen noch die beiden $\frac{4D}{m^2}=2$, 1 hinzutreten müssten; aber eine genauere Betrachtung zeigt, dass sie beide nicht statthaben können. Aus der ersten Annahme würde fliessen $\frac{4AC}{m^2}-\frac{4B^2}{m^2}=2$, woher $\left(\frac{2B}{m}\right)^2\equiv-2\ (\mathrm{mod}\ 4)$, und ebenso würde man aus der zweiten Annahme erhalten $\left(\frac{2B}{m}\right)^2\equiv-1\ (\mathrm{mod}\ 4)$. Beide Congruenzen können aber nicht bestehen, weil -2 und -1 quadratische Nichtreste des Moduls 4 sind.

Beispiel 1. Betrachten wir die beiden Formen $(A, B, C) = (1, 0, 1)$ und (M, z, s), wo M irgend eine durch die Form $(1, 0, 1)$ darstellbare Zahl bezeichnet und die Grössen z und s ihre Bestimmung durch die Bedingungsgleichung $z^2+1 = Ms$ erhalten. Aus der letzteren erhellt sofort, dass, damit die untersuchte Repräsentation möglich sei, nothwendig -1 ein quadratischer Rest von M sein müsse; mithin können nur solche Zahlen durch die Form x^2+y^2 dargestellt werden, welche unter der allgemeinen Zahlform $M = 4n+1$ stehen, und eine Zahl, wie $4n-1$, gestattet überhaupt nicht die Zerfällung in zwei Quadrate. Es lässt sich aber nun weiter beweisen, dass für eine derartige Zerfällung die eben bezeichnete (die Zahlform von M betreffende) Bedingung nicht blos nothwendig, sondern auch hinreichend sei. Von welcher Beschaffenheit nämlich die Form (M, z, s) auch sein möge, sie hat stets die Determinante -1 und kann, wenn M positiv und z als eine kleinste Wurzel der obigen Bedingungsgleichung bestimmt ist, nur positive Zahlen darstellen; nun existirt aber nur eine einzige reducirte Form, welche diese Determinante hat und positive Zahlen darzustellen fähig ist, nämlich $(1, 0, 1)$; mithin sind die beiden Formen $(1, 0, 1)$ und (M, z, s) einander (im eigentlichen Sinne) aequivalent. Daraus erhellt die Möglichkeit eine solche Reihe angrenzender Formen zu bilden, vermöge deren eine Transformation der ersten Form in die zweite gefunden werden kann. Sei diese Transformation $x = \alpha\xi+\beta\eta$ und $\eta = \gamma\xi+\delta\eta$, so handelt es sich darum, alle übrigen davon verschiedenen Transformationen zu bestimmen. Da im gegenwärtigen Falle die Grösse m der Einheit gleich ist, so kommt die Hülfsgleichung $t^2+Du^2=m^2$ auf die Gestalt $t^2+u^2=1$ und man hat $\frac{4D}{m^2}=4$, d. h. es tritt der Fall b) ein. Wir bekommen daher folgende 4 Lösungen der Gleichung $x^2+y^2=M$: $x=\alpha$, $y=\gamma$; $x=-\alpha$, $y=-\gamma$; $x=-\gamma$, $y=\alpha$; $x=\gamma$, $y=-\alpha$.

Die genannten Repräsentationen von M durch $(1, 0, 1)$ sind aber nur diejenigen, welche einer speciellen und in den kleinsten Zahlen ausgedrückten Lösung der Gleichung $z^2+1=Ms$ nach z und s zugehören, nämlich dem Lösungssysteme $z=+\zeta$, $s=\sigma$, und, wie auch die Zahl M beschaffen sein möge, so werden immer noch 4 andere Repräsentationen existiren, welche dem entgegengesetzten Lösungssysteme $z=-\zeta$, $s=\sigma$

verknüpft oder liirt sind; dieselben sind: $x=\alpha$, $y=-\gamma$; $x=-\alpha$, $y=\gamma$; $x=\gamma$, $y=\alpha$; $x=-\gamma$, $y=-\alpha$ und werden aus den vorhergehenden erhalten durch Vertauschung von γ mit $-\gamma$. Dies erhellt sofort aus der Bemerkung, dass, da die Form (1, 0, 1) eine zweideutige ist, sie ebensowohl der Form (M, ζ, σ), wie der Form (M, $-\zeta$, σ) im eigentlichen Sinne aequivalent sein muss und mithin die Transformation $x=\alpha\xi-\beta\eta$, $y=-\gamma\xi+\delta\eta$, vermöge derer (1, 0, 1) in (M, $-\zeta$, σ) übergeht, gleichfalls in Betracht kommt.

Ist nun M eine Primzahl oder die Potenz einer solchen, so existiren ausser den beiden Lösungen $z=\pm\zeta$, $s=\sigma$ der Bedingungsgleichung keine, die davon verschieden sind, und es sind die aufgezählten 8 Repräsentationen von M durch (1, 0, 1) die einzig möglichen. Alle diese geben aber dieselbe Zerfällung von M in zwei Quadrate, weil sie mit den verschiedenen Variationen zusammenfallen, welche der Ausdruck $(\pm\alpha)^2+(\pm\gamma)^2$ in Rücksicht auf die Ordnung der Summanden und die Wahl der Vorzeichen zulässt.

Ist dagegen M eine zusammengesetzte Zahl der Form $4n+1$ und aus lauter Primzahlen von eben dieser Form zusammengesetzt, so hat, wenn k die Anzahl der ungleichen in M hineingehenden Primfactoren bezeichnet, die Gleichung $z^2+1=Ms$ 2^n von einander verschiedene und zu je zwei einander entgegengesetzte Lösungssysteme; mithin giebt es 2^{n-1} von einander verschiedene Zerfällungen der Zahl M in zwei Quadrate. — Wenn irgend ein Primfactor von M die Form $4n-1$ hat, so ist -1 ein Nichtrest von M und dem zu Folge M überhaupt nicht durch einen Ausdruck von der Form x^2+y^2 darstellbar.

Wenn M endlich eine gerade Zahl, so ist die Gleichung $z^2+1=Ms$, oder, was dasselbe sagt, die Congruenz $z^2\equiv-1 \pmod M$ nur dann möglich, wenn $\frac{M}{2}$ eine ungerade Zahl ist und sich aus lauter Primfactoren von der Form $4n+1$ zusammensetzt; sei die Anzahl der ungleichen Primfactoren von $\frac{M}{2}$ gleich k, so giebt es wieder 2^{k-1} verschiedene Zerfällungen von M in zwei Quadrate.

Die vorstehenden Erörterungen beziehen sich auf lauter solche Repräsentationen, in denen x und y relative Primzahlen zu einander sind, also keinen die Einheit übertreffenden gemeinschaftlichen Theiler besitzen.

Wenn wir einen solchen Theiler gestatten, so wissen wir, dass M mindestens einen von 1 verschiedenen quadratischen Factor einschliessen muss. Dies vorausgesetzt sei μ^2 irgend ein quadratischer Factor von M, so hat man sich die Gleichung $x'^2+y'^2=\frac{M}{\mu^2}$ in relativen Primzahlen für x' und y' aufzulösen: so wird die gesuchte Repräsentation von M durch (1, 0, 1) erhalten durch das Werthsystem $x=\mu x'$ und $y=\mu y'$. Damit dies möglich sei, ist nothwendig und zureichend, dass $\frac{M}{\mu^2}$ eine Zahl sei, die den vorher auseinandergesetzten Bedingungen genügt, d. h. wenn sie gerade ist, sich weder durch 4, noch durch irgend einen Factor von der Form $4n-1$ theilen lasse, und wenn sie ungerade ist, gleichfalls keinen Factor von der Form $4n-1$ enthalte.

Sei z. B. $M=20$, so ist $\mu^2=4$, $x'^2+y'^2=5$ und $x'=1$, $y'=2$, mithin $x=2$, $y=4$, also die gesuchte Zerfällung $20=4+16$ und sonst keine mehr. Sei $M=180$, so hat man $\mu^2=4$, 9, 36 und dem entsprechend $x'^2+y'^2=45$, 20, 5; die beiden ersten Gleichungen sind (in relativen Primzahlen für x' und y') unmöglich, die letzte giebt $x'=1$, $y'=2$, also $x=6$, $y=12$. Sei schliesslich $M=36$, so ist $\mu=4$, 9, 36 und $x'^2+y'^2=9$, 4, 1. Die beiden ersten Gleichungen sind wieder in relativen Primzahlen für x' und y' nicht auflösbar; die letzte giebt $x'=0$, $y'=1$ (wo 0 und 1 als relative Primzahlen gelten, weil sie durch keine Zahl über 1 beide zugleich ohne Rest theilbar sind), also $x=0$, $y=6$.

In der vorhergehenden Analyse ist unter Anderem folgendes elegante Theorem enthalten: Jede Primzahl der Form $4n+1$ kann in die Summe zweier Quadrate und zwar nur auf eine einzige Art zerfällt werden.

Beispiel 2. Betrachten wir die Repräsentation $x^2+2y^2=M$ unter der Voraussetzung, dass M eine absolute Primzahl und demzufolge x und y relative Primzahlen zu einander seien, so ist dieselbe überhaupt unmöglich, wenn -2 ein quadratischer Nichtrest von M ist, dagegen immer möglich, wenn -2 ein quadratischer Rest von M ist. In der That seien die Grössen z und s durch die Gleichung $z^2+2=Ms$ bestimmt, so ist die Form (M, z, s) der Form (1, 0, 2) nothwendig aequivalent, weil (1, 0, 2) die einzige reducirte Form für die Determi-

nante —2 ist, welche eine positive Zahl ausdrücken kann. Also ist einmal der grösste gemeinschaftliche Theiler zwischen M, z, s derselbe, wie zwischen 1, 0, 2, d. h. er ist $m=1$ und dann existirt eine in bekannter Weise bestimmbare Transformation von (1, 0, 2) in (M, z, s). Sei dieselbe $x=\alpha\xi+\beta\eta$, $y=\gamma\xi+\delta\eta$, so hat man wegen der Gleichung $\frac{4D}{m^2}=8$ den Fall a) und mithin sind die beiden Repräsentationen von M, welche zu der Lösung $z=\zeta$ und $s=\sigma$ unserer Hülfsgleichung gehören, durch die beiden Werthsysteme $x=\alpha$, $y=\gamma$ und $x=-\alpha$, $y=-\gamma$ gegeben. Da die Form (1, 0, 2) eine zweideutige ist, so kommen noch dazu die Werthsysteme $x=\alpha$, $y=-\gamma$ und $x=-\alpha$, $y=\gamma$, welche zu der entgegengesetzten Lösung $z=-\zeta$ und $s=\sigma$ der Hülfsgleichung gehören. Man folgert hieraus leicht das folgende Theorem: **Jede Primzahl von einer der Formen $8n+1$ oder $8n+3$ gestattet eine und nur eine Zerfällung in die Summe eines Quadrates und eines Doppelquadrates.**

Beispiel 3. Betrachten wir die Form x^2+7y^2, so kann dieselbe nur solche Primzahlen M darstellen, die zum quadratischen Reste —7 haben; diese Bedingung ist aber nicht nur nothwendig, sondern auch zureichend. Sei nämlich wieder $z^2+7=Ms$, so ist die Form (M, z, s) nothwendig mit der Form (1, 0, 7) aequivalent; denn die beiden einzigen reducirten Formen mit der Determinante —7, welche eine positive Zahl darstellen können, sind x^2+7y^2 und $2x^2+2xy+4y^2$ und einer von diesen beiden muss die Form (M, z, s) aequivalent sein. Denken wir uns nun irgend ein speciell bestimmtes M, für welches (M, z, s) der Form (2, 1, 2) aequivalent sein könnte, so müsste die Zahl M darstellbar sein durch die letztere Form, d. h. es müsste M eine gerade Zahl sein im Widerspruche zur Voraussetzung. Also sind nothwendig die Formen (1, 0, 7) und (M, z, s) einander aequivalent. Da wir $\frac{4D}{m^2}=\frac{28}{1}=28$, also >4 haben, so tritt wieder der Fall a) ein und man hat das Theorem:

Alle Primzahlen, von denen —7 ein quadratischer Rest ist, gestatten eine und nur eine Zerfällung in ein Quadrat und das Siebenfache eines Quadrates.

Beispiele sind: $33=4^2+7.1^2$, $29=1+7.2^2$, $37=9+7.2^2$, $43=6^2+7.1^2$, $53=25+7.2^2$, $67=2+7.3^2$ u. s. w.

2) Auflösung der Gleichung $t^2-Du^2=m^2$, wenn die Determinante D positiv und ein vollständiges Quadrat $=h^2$ ist. Alsdann existiren die beiden Lösungssysteme $t=m$, $u=0$ und $t=-m$, $u=0$ und ausser diesen keine weiter. Nehmen wir nämlich das System der Werthe $u=u'$ und $t=t'$ als eine zweite Lösung an, so folgt $4t'^2-4Du'^2=4m^2$ und da $4D$ durch m^2 theilbar ist, so muss auch $4t'^2$ durch m^2 ohne Rest sich theilen lassen und man erhält, indem man für D seinen Werth h^2 einsetzt und durch m^2 dividirt, die Gleichung $\left(\frac{2t'}{m}\right)^2-\left(\frac{2hu'}{m}\right)^2=4$, so dass jedes Glied links eine ganze Zahl bezeichnet. Wenn aber die Differenz zweier Quadrate gleich 4 sein soll, so muss nothwendig das kleinere gleich 0 sein; daraus ergiebt sich $u'=0$, $t'=\pm m$, d. h. das hypothetische Lösungssystem fällt mit den beiden gegebenen zusammen oder es existiren nur diese und sonst keine mehr.

Dieses vorausgesetzt seien wieder (A, B, C) und (M, n, s) aequivalente Formen und $x=\alpha\xi+\beta\eta$, $y=\gamma\xi+\delta\eta$ eine Transformation der ersten in die letzte; alsdann hat man noch die zweite Transformation $x=-\alpha\xi-\beta\eta$, $y=-\gamma\xi-\delta\eta$ und ausserdem keine mehr; mithin existiren nur zwei und nicht mehr Repräsentationen von M durch (A, B, C), welche zu einer speciellen Lösung der Hülfsgleichung $z^2-h^2=Ms$ gehören; denselben entsprechen die Werthsysteme $x=\pm\alpha$, $y=\pm\gamma$.

3) Auflösung der Gleichung $t^2-Du^2=m^2$, wenn D eine positive Zahl bezeichnet, die kein vollständiges Quadrat ist.

In diesem Falle existiren eine unendliche Menge von Auflösungen (wenn nämlich solche überhaupt möglich sind) und wir bemerken zur Vereinfachung des Geschäftes ihrer Aufsuchung, dass, wenn $t=T$ und $u=U$ ein System positiver und die Gleichung befriedigender Zahlenwerthe bezeichnen, aus dieser einen Lösung sich sofort drei andere ergeben, nämlich $t=T$ und $u=-U$, $t=-T$ und $u=U$, $t=-T$ und $u=-U$. Demgemäss ist es ausreichend alle möglichen verschiedenen Lösungssysteme aufzustellen, in denen t und u positive ganze Zahlen bezeichnen und wir wollen unter diesen zunächst dasjenige uns bestimmen, in wel-

chem u, abgesehen von dem schon bekannten Lösungssysteme $t = m$ und $u = 0$, den kleinsten Werth hat.

Die Gleichung $t^2 - Du^2 = m^2$ ist zu Folge der Anlage unserer Untersuchung eng verknüpft mit den beiden aequivalenten Formen (A, B, C) und (M, z, s). Sobald diese Formen bestimmt und als aequivalente nachgewiesen sind, so existiren, wie man aus dem Schlussbeispiel zu §. 24 sieht und auch aus der Periodicität der reducirten Formen mit positiver Determinante in allgemeiner Weise folgern darf, eine unendliche Menge von Transformationen der Form (A, B, C) in die Form (M, z, s); da nun, in Uebereinstimmung mit §. 26, je zwei derselben eine Lösung unserer Gleichung nach t und u bestimmen, so folgt mit Nothwendigkeit, dass die Zahl der Auflösungen unendlich ist. Zugleich ist der Gang, den wir Behufs ihrer Auflösung einzuschlagen haben, durch diese Betrachtung vorgeschrieben.

Wir werden uns vermöge einer Reihe von angrenzenden Formen die reducirte Form zu (A, B, C) suchen; sei dieselbe $f = (a, b, -a')$ und nehmen wir in Analogie mit der §. 24. unter 2) und 3) eingeführten Bezeichnung an, dass ihre Periode aus n Formen bestehe und mithin durch die Reihe $f, f_1, f_2, f_3, \ldots\ldots f_{n-1}$ dargestellt werde, so ist die in der genannten Reihe auf f_{n-1} folgende Form f_n identisch mit f und man wird nach vorhergegangener Bestimmung der Partialquotienten $h_1, h_2, h_3, \ldots. h_n$ sich in bekannter Weise eine Transformation von f in f_n bilden können, nämlich $x = \alpha_n x_n + \beta_n y_n$, $y = \gamma_n x_n + \delta_n y_n$. Nun ist, wegen der zwischen den Formen f und f_n bestehenden Identität, eine zweite Transformation $x = 1 . x_n + 0 . y_n$, $y = 0 . x_n + 1 . y_n$. Aus diesen beiden Transformationen ergiebt sich, wenn wir die Formeln (18) und (19) des §. 26. anwenden und zwar für $\alpha = \delta = 1$, $\beta = \gamma = 0$, $\alpha' = \alpha_n$, $\beta' = \beta_n$, $\gamma' = \gamma_n$, $\delta' = \delta_n$ das folgende Lösungssystem der Gleichung $t^2 - Du^2 = m^2$:

$$T = \frac{(\alpha_n + \delta_n)m}{2}, \quad U = \frac{\gamma_n . m}{a}.$$

Uebrigens ist es nicht gerade nothwendig, die reducirte Form $f = (a, b, -a')$, welche sich durch die Form (A, B, C) ergiebt, bei dieser Entwickelung zu benutzen, sondern man könnte an ihrer Stelle auch jede reducirte Form, wie $\varphi = (A', B', C')$ wählen von der Beschaffenheit, dass m der grösste gemeinschaftliche Theiler zwischen A', $2B'$ und C' sei.

Diese Beschaffenheit ist hier wesentlich und kommt, wenn sonst keine derartige Form existirt, zum Mindesten der Form $(a, b, -a')$ zu. Denn der Zusammenhang zwischen der Form (A, B, C) und der Gleichung $t^2 - Du^2 = m^2$ besteht ja nach der einen Seite darin, dass m der grösste gemeinschaftliche Divisor zwischen A, $2B$, C sei; also muss m auch der grösste gemeinschaftliche Divisor zwischen den Coefficienten a, $2b$, a' der aequivalenten Form $f = (a, b, -a')$ sein.

Mag nun die Form $f = (a, b, -a')$ eine vermöge der Form (A, B, C) hergeleitete sein oder irgend eine beliebige reducirte, deren Coefficienten m zum grössten gemeinschaftlichen Maasse haben — es lässt sich in beiden Fällen darthun, dass der auf die angegebene Weise hergeleitete Werth $u = U$ der kleinste unter allen Zahlenwerthen von u ist, welche von 0 verschieden sind und der Gleichung $t^2 - Du^2 = m^2$ Genüge leisten.

Nehmen wir irgend einen von 0 und U verschiedenen Werth $u = u'$ an, der die Fähigkeit hat, den Ausdruck $m^2 + Du^2$ zu einem vollständigen Quadrate zu machen und sei der correspondirende Werth von t gleich t'. Dieses neue Werthsystem muss irgend einer Transformation der Form f in die Form f_n, d. h. in sich selbst entsprechen. Bezeichnen wir die Unbestimmten dieser beiden Formen respective mit X, Y und x, y, so wird diese Transformation erhalten aus der einen bekannten Transformation $X = 1.x + 0.y$, $Y = 0.x + 1.y$ und dem eben bezeichneten Lösungssysteme; wir haben zu dem Zwecke nur nöthig in den Formeln (24) des vorigen Paragraphen an Stelle der Grössen A, B, C, α, β, γ, δ, U, T respective a, b, $-a'$, 1, 0, 0, 1, u', t' zu setzen; dieselben gehen dadurch über in:

$$X = \frac{t' - bu'}{m} x + \frac{a'u'}{m} y, \quad Y = \frac{au'}{m} x + \frac{t' + bu'}{m} y.$$

Gehen wir jetzt auf das früher erörterte Theorem zurück, dass, wenn zwei reducirte Formen mit positiver Determinante einander aequivalent sind, nothwendig jede von ihnen in der Periode der anderen enthalten sei, so folgt aus der Natur des daselbst geführten Beweises, dass, wenn zwei aequivalente Formen $f = (a, b, -a')$ und $F = (A, B, -A')$, von denen die letzte gegenwärtig als der ersten identisch anzusehen ist, so dass man $A = a$, $B = b$, $A' = a'$ hat, durch irgend eine gegebene Transfor-

mation in einander übergehen, diese Transformation entweder mit geradezu denselben oder mit entgegengesetzten Werthen der Coefficienten unter allen Umständen in der Reihe von Transformationen sich vorfindet, vermöge derer die Form f in irgend eine Form der Reihe

$$\ldots\ldots f_{-4},\ f_{-3},\ f_{-2},\ f_{-1},\ f,\ f_1,\ f_2,\ f_3,\ \ldots\ldots f_{n-1},\ f_n,\ f_{n+1},\ \ldots\ldots$$

übergeht. Diese gegebene Transformation war dort dargestellt durch $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$ und hier haben wir für α', β', γ', δ' die specielle Bestimmung $\alpha' = \frac{t' - b'u'}{m}$, $\beta' = \frac{a'u'}{m}$, $\gamma' = \frac{au'}{m}$, $\delta' = \frac{t' + bu'}{m}$, mithin $\frac{\alpha'}{\gamma'} = \frac{t' - bu'}{au'}$, $\frac{\beta'}{\delta'} = \frac{a'u'}{t' + bu'}$. Nun können zwei Fälle möglicher Weise eintreten. Es kann entweder a dasselbe Vorzeichen haben, wie $\frac{\alpha'}{\gamma'}$ und dann ist die gegebene Transformation, welche wir betrachten, identisch mit der Transformation von f in irgend eine bestimmte Form der Periode mit positivem Index: oder a hat ein anderes Vorzeichen als $\frac{\alpha'}{\gamma'}$ und dann ist die betrachtete Transformation identisch mit der Transformation von f in irgend eine bestimmte Form seiner Periode mit negativem Index. Hier tritt mit Bestimmtheit nur der erste unter den gedachten beiden Fällen ein. Denn aus der Gleichung $t'^2 - Du'^2 = m^2$ folgt, wenn man für D seinen Werth substituirt, $t'^2 - b^2u'^2 = aa'u'^2m^2$, mithin, da a und a' Grössen von dem nämlichen Vorzeichen sind, $t'^2 - b^2u'^2$ oder $(t' - bu')(t' + bu') > 0$. Da nun t', b', u' als wesentlich positive Zahlen angenommen werden müssen, so kann diese Ungleichung nur bestehen, wenn $t' - bu'$ und folglich auch $\frac{t - bu'}{u'}$ eine positive Grösse ist. Daraus erhellt aber unmittelbar, dass die Grössen a und $\frac{\alpha'}{\gamma'} = \frac{t' - bu'}{au'}$ gleiches Zeichen haben.

Die eben zu Ende geführte Betrachtung liefert den Beweis, dass die in Rede stehende Transformation

$$X = \frac{t' - bu'}{m} x + \frac{a'u'}{m} y,\quad Y = \frac{au'}{m} x + \frac{t' + bu'}{m} y$$

zusammenfällt mit der Transformation von f in irgend eine specielle Form der Reihe:

$$f,\ f_1,\ f_2,\ f_3,\ f_4,\ \ldots\ldots f_{n-1},\ f_n,\ f_{n+1},\ \ldots\ldots$$

und zwar unter der Voraussetzung, dass diese Transformation nach dem in §. 24. unter 3) auseinandergesetzten Gesetze vermöge Verwandlung von $\frac{\sqrt{D}-b}{a}$ in einen Kettenbruch gebildet werden. Sei diese Form allgemein bezeichnet durch f_m, so giebt die Bedingung, dass unsere Transformation eine mit f identische Form erzeugen soll, die Congruenz $m \equiv 0 \pmod{n}$. Nun kann m nicht gleich 0 sein; denn dieser Annahme entspräche die Transformation $X = 1 \,.\, x + 0 \,.\, y$, $Y = 0 \,.\, x + 1 \,.\, y$, welche mit der obigen nur dann identisch werden kann, wenn man gegen die Voraussetzung $u' = 0$ hat. Ebensowenig kann $m = n$ sein; denn diese Annahme entspräche der Transformation $X = \alpha_n x + \beta_n y$, $Y = \gamma_n x + \delta_n y$, welche mit der obigen nur dann identisch werden kann, wenn man $\beta_n = \frac{a'u'}{m}$, $\gamma_n = \frac{au'}{m}$ hat. Die letzte dieser Gleichungen giebt aber mit der obigen Bestimmungsgleichung für U, nämlich $U = \frac{\gamma_n \,.\, m}{a}$ multiplicirt gegen die Voraussetzung $U = u'$. Also, da m nur positiv angenommen werden und weder gleich 0, noch gleich n sein darf, ist es nothwendig ein Multiplum von n grösser als n oder mit anderen Worten, unsere Transformation ist die Transformation von f in eine specielle unter den Formen f_{2n}, f_{3n}, f_{4n}, f_{5n}, ... Sei die betreffende Form $f_{n+\varrho n}$, wo ϱ eine von 0 verschiedene positive ganze Zahl bezeichnet, so hat man die Transformation $X = \alpha_{n+\varrho n} x + \beta_{n+\varrho n} y$, $Y = \gamma_{n+\varrho n} x + \delta_{n+\varrho n} y$ und aus dieser zieht man wiederum durch Vergleichung mit der oben aufgestellten damit identischen die Gleichung $\gamma_{n+\varrho n} = \frac{au'}{m}$. Nun ist aber $U = \frac{\gamma_n \,.\, m}{a}$, also durch Multiplication $U = \frac{\gamma_n}{\gamma_{n+\varrho n}} \,.\, u'$, woher $U < u'$ folgt; denn die Grössen γ wachsen, wie wir wissen, mit wachsenden Indices. Also ist U kleiner als jeder positive von 0 verschiedene Zahlenwerth der Grösse u, welcher der Gleichung $t^2 - Du^2 = m^2$ Genüge leistet, d. h. er ist, mit Ausschluss des Werthes $u = 0$, der kleinste unter allen nur möglichen.

Rücksichtlich der Auffindung dieser kleinsten Wurzel u bemerken wir, dass wir immer eine solche reducirte Form $(a, b, -a')$ dazu benutzen können, in welcher der Coefficient a eine positive Grösse ist; denn sollte a negativ sein, so brauchte man nur die umgekehrte Form

$(-a', b, a)$ anzuwenden, welche dann eine reducirte Form mit positivem ersten Exponenten sein wird. Dies vorausgesetzt ist in den Entwickelungen des §. 24. unter 2) und 3) der Beweis enthalten, dass die Aufsuchung der Transformation von f in f_n, d. h. die Bestimmung der Grössen α_n, β_n, γ_n, δ_n auf die Entwickelung der Irrationalgrösse $\frac{\sqrt{D}-b}{a}$ in einen unendlichen Kettenbruch hinausläuft, dass dieser Kettenbruch periodisch ist und dass die Periode der Partialquotienten durch die Reihe der Zahlen:

$$h_1, h_2, h_3, h_4, \ldots\ldots h_{n-1}, h_n,$$

wo n eine gerade Zahl sein muss, gebildet wird. Bezeichnen wir jetzt die Näherungswerthe von $\frac{\sqrt{D}-b}{a}$, die diesen Partialquotienten entsprechen, der Reihe nach durch

$$\frac{0}{1}\ \frac{Z_1}{N_1}, \frac{Z_2}{N_2}, \frac{Z_3}{N_3}, \frac{Z_4}{N_4}, \ldots\ldots \frac{Z_{n-1}}{N_{n-1}}\ \frac{Z_n}{N_n}$$

und bildet sich aus der Folge sämmtlicher Zähler und aus der Folge sämmtlicher Nenner die beiden Reihen von mit Vorzeichen versehenen Zahlen

$$\begin{array}{cccccccc} +0 & -Z_1 & -Z_2 & +Z_3 & +Z_4 & -Z_5 & -Z_6 & \ldots\ldots \\ +1 & -N_1 & -N_2 & +N_3 & +N_4 & -N_5 & -N_6 & \ldots\ldots, \end{array}$$

so sind die Vorzeichen, welche den 4 Grössen Z_{n-1}, Z_n, N_{n-1}, N_n zukommen, für alle durch das Zeichen des Ausdruckes $(-1)^{\frac{n}{2}}$ bestimmt und die Transformation von f in f_n wird dargestellt durch die Formeln $X = (-1)^{\frac{n}{2}} Z_{n-1} x + (-1)^{\frac{n}{2}} Z_n y$, $Y = (-1)^{\frac{n}{2}} N_{n-1} x + (-1)^{\frac{n}{2}} N_n y$, also haben wir in den obigen Formeln für T und U an Stelle von α_n, β_n, γ_n, δ_n der Reihe nach die Grössen $(-1)^{\frac{n}{2}} Z_{n-1}$, $(-1)^{\frac{n}{2}} Z_n$, $(-1)^{\frac{n}{2}} N_{n-1}$, $(-1)^{\frac{n}{2}} N_n$ zu substituiren und bekommen dadurch $T = (-1)^{\frac{n}{2}} \frac{(Z_{n-1}+N_n)m}{2}$, $U = (-1)^{\frac{n}{2}} \frac{N_{n-1} \cdot m}{a}$. Hierbei ist hinsichtlich des Index n, welcher angiebt, wieviel Glieder die Periode der Partialquotienten $-h_1$, $-h_2$, $+h_3$, $-h_4$, ... hat, noch die Bemerkung zu machen, dass er mit der Anzahl der Glieder, welche die Periode des Kettenbruches hat, nur für den Fall, dass dieselbe gerade ist, identisch ist; dagegen, wenn diese Anzahl eine ungerade ist, so ist der Index n genau das Doppelte derselben; d. h. einer Periode der h_1, $-h_2$, h_3, $-h_4$, ... $-h_n$ entsprechen zwei Perioden des

Kettenbruches. Es hängt dieses mit dem Satze zusammen, dass die Periode einer reducirten Form immer aus einer geraden Anzahl von Formen sich zusammensetzt. Dieses vorausgesetzt, da es nur auf die absoluten Zahlenwerthe von T und U ankommt, können wir folgende praktische Regel zur Bestimmung der genannten Grössen geben:

Man suche sich eine solche reducirte Form $(a, b, -a')$ zu bestimmen, in der a positiv und m das grösste gemeinschaftliche Mass von a, $2b$, a' ist; hierauf verwandele man sich den Ausdruck $\frac{\sqrt{D}-b}{a}$ in einen Kettenbruch, bestimme sich dessen Periode und suche, je nachdem die Periode eine gerade oder ungerade Anzahl von Gliedern enthält, diejenigen Näherungswerthe, welche den beiden letzten Partialquotienten der ersten oder zweiten Periode entsprechen. Seien dieselben respective $\frac{Z_{n-1}}{N_{n-1}}$ und $\frac{Z_n}{N_n}$, so ist der kleinste Werth von u, der der Gleichung $t^2-Du^2=m^2$ Genüge leistet, in dem Lösungssysteme enthalten:

$$T=\frac{(Z_{n-1}+N_n)m}{2},\quad U=\frac{N_{n-1}\cdot m}{a},$$

Die Verwandlung von $\frac{\sqrt{D}-b}{a}$ in einen Kettenbruch ist aus den Elementen her bekannt; ohnedem ist sie factisch in der Entwickelung des §. 24. unter 3) zur Darstellung gekommen. Es wird daher ausreichend sein an einem Beispiele den Gang der Rechnung zu zeigen. Sei die aufzulösende Gleichung $t^2-79u^2=1$, also $D=79$, $m=1$, so ist eine reducirte Form, wie wir sie gebrauchen, die Form $(3, 8, -5)$, dieselbe, welche bereits in der oben citirten Nummer als Beispiel gedient hat. Mit der dortigen Rechnung mag daher das folgende Schema verglichen werden:

$$\frac{\sqrt{D}-b}{a}=\frac{\sqrt{79}-8}{3}=\frac{1}{h_1},\quad h_1=\frac{3}{\sqrt{79}-8}=\frac{\sqrt{79}+8}{5}=3+\frac{1}{h_2},$$

$$h_2=\frac{5}{\sqrt{79}-7}=\frac{\sqrt{79}+7}{6}=2+\frac{1}{h_3},$$

$$h_3=\frac{6}{\sqrt{79}-5}=\frac{\sqrt{79}+5}{9}=1+\frac{1}{h_4},$$

$$h_4 = \frac{9}{\sqrt{79}-4} = \frac{\sqrt{79}+4}{7} = 1 + \frac{1}{h_5},$$

$$h_5 = \frac{7}{\sqrt{79}-3} = \frac{\sqrt{79}+3}{10} = 1 + \frac{1}{h_6},$$

$$h_6 = \frac{10}{\sqrt{79}-7} = \frac{\sqrt{79}+7}{3} = 5 + \frac{1}{h_7},$$

$$h_7 = \frac{3}{\sqrt{79}-8} = h_1.$$

Also ist $\frac{\sqrt{79}-8}{3} = \frac{1}{3+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{5+}\frac{1}{3+}\frac{1}{2+}\ldots\ldots$

	3	2	1	1	1	5
$\frac{0}{1}$	$\frac{1}{3}$	$\frac{2}{7}$	$\frac{3}{10}$	$\frac{5}{17}$	$\frac{8}{27}$	$\frac{45}{152}$

$Z_{n-1} = 8$, $N_n = 152$,
$Z_n = 45$, $N_{n-1} = 27$.

$$T = \frac{(8+152).1}{2} = 80, \quad U = \frac{27.1}{3} = 9.$$

Als ein zweites Beispiel wollen wir die Gleichung $t^2 - 29u^2 = m^2$ betrachten. Die reducirte Form (1, 5, —4) genügt allen geforderten Eigenschaften. Bilden wir uns ihre Periode, nämlich:

(1, 5, —4), (—4, 3, 5), (5, 2, —5), (—5, 3, 4), (4, 5, —1),
(—1, 5, 4), (4, 3, —5), (—5, 2, 5), (5, 3, —4), (—4, 5, 1);

so erkennt man, dass die Periode der h_1, $-h_2$, h_3, $-h_4$, ... h_n folgende ist:

—2 +1 —1 +2 —10 +2 —1 +1 —2 +10

und in Uebereinstimmung mit der obigen Bemerkung entsprechen dieser Periode zwei Perioden des Kettenbruches:

$$\frac{\sqrt{D}-b}{a} = \sqrt{29}-5 = \frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{2+}\frac{1}{10+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{2+}\frac{1}{10+}\ldots\ldots$$

Die weitere Rechnung macht sich, wie folgt:

	2	1	1	2	10	2	1	1	2	10
$\frac{0}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{2}{5}$	$\frac{5}{13}$	$\frac{52}{135}$	$\frac{109}{283}$	$\frac{161}{418}$	$\frac{270}{701}$	$\frac{701}{1820}$	$\frac{7280}{18901}$

$$T = \frac{701+18901}{2} = 9801, \quad U = 1820.$$

Benutzte man statt der Näherungswerthe, welche den beiden letzten Partialquotienten der zweiten Periode entsprechen, diejenigen, welche den beiden letzten Partialquotienten der ersten Reihe entsprechen, so erhielte man

$$T' = \frac{5+135}{2} = 70, \quad U' = 13$$

und dies System von Zahlenwerthen löst zwar nicht die vorgelegte Gleichung auf, wohl aber die damit nahe verwandte $t^2 - 29u = -1$.

Wenn man will, kann man die Berechnung noch mehr vereinfachen durch Aufstellung solcher Formeln für T and U, deren Berechnung nur entweder die Nenner oder die Zähler der beiden erwähnten Näherungswerthe voraussetzt. Zu diesem Zwecke schreiben wir uns die Formeln (18), (19), (20), (21) des §. 26, indem wir für c, α, β, γ, δ, α', β', γ', δ' respective die Grössen $-a'$, 1, 0, 0, 1, α_n, β_n, γ_n, δ_n einführen, wie folgt um:

$$2T = (\alpha_n + \delta_n).m,$$

$$aU = \gamma_n m, \quad 2bU = (\delta_n - \alpha_n)m, \quad a'U = \beta_n m.$$

Multipliciren wir die zweite dieser Gleichungen mit $2b$, die dritte mit a, so ergiebt sich $2b\gamma_n = a(\delta_n - \alpha_n)$ und wenn man die dritte mit a', die vierte mit $2b$ multiplicirt, $a'(\delta_n - \alpha_n) = 2b\beta_n$. Hieraus folgt $\alpha_n = \delta_n - \frac{2b}{a}\gamma_n$ und $\delta_n = \frac{2b}{a'}\beta_n + \alpha_n$. Setzt man diese beiden Werthe in die erste Gleichung ein, so kann man sich ersichtlich folgende beiden verschiedenen Gleichungssysteme für T und U zusammenstellen:

$$2T = \left(2\delta_n - \frac{2b}{a}\gamma_n\right)m, \quad aU = \gamma_n m$$

$$2T = \left(2\alpha_n + \frac{2b}{a'}\beta_n\right)m, \quad a'U = \beta_n m$$

und setzt man jetzt für α_n, β_n, γ_n, δ_n ihre absoluten Werthe Z_{n-1}, Z_n, N_{n-1}, N_n ein, wodurch, da die 4 genannten Coefficienten alle 4 gleiches

Zeichen haben, der absolute Werth von T und U ungeändert bleibt, so bekommen wir folgende beiden Systeme von Formeln für T und U:

$$T=\left(N_n-\frac{b}{a}N_{n-1}\right)m,\quad U=\frac{N_{n-1}\,.\,m}{a};$$

$$T=\left(Z_{n-1}+\frac{b}{a}Z_n\right)m,\qquad U=\frac{Z_n\,.\,m}{a}.$$

Gehen wir jetzt weiter in unserer Untersuchung und zeigen, wie man aus der kleinsten positiven Lösung der Gleichung $t^2-Du^2=m^2$ alle übrigen sich herleiten könne. Zu dem Zwecke gebe man dieser Gleichung die Form $\left(\frac{T}{m}+\frac{U}{m}\sqrt{D}\right)^e\left(\frac{T}{m}-\frac{U}{m}\sqrt{D}\right)^e=1$, wo e irgend eine beliebige positive ganze Zahl bezeichnet und setze grösserer Kürze halber

$$\frac{m}{2}\left(\frac{T}{m}+\frac{U\sqrt{D}}{m}\right)^e+\frac{m}{2}\left(\frac{T}{m}-\frac{U\sqrt{D}}{m}\right)^e=t_e$$

$$\frac{m}{2\sqrt{D}}\left(\frac{T}{m}+\frac{U\sqrt{D}}{m}\right)^e-\frac{m}{2\sqrt{D}}\left(\frac{T}{m}-\frac{U\sqrt{D}}{m}\right)^e=u_e,$$

so dass t_e und u_e die respectiven Werthe bezeichnen, welche die Ausdrücke linker Hand für die verschiedenen Werthe von e annehmen. Setzen wir hier für e nach und nach die Zahlen 0, 1, 2, 3, 4, ... in infin. ein, so erhalten wir die Werthsysteme t_0 und u_0, t_1 und u_1, t_2 und u_2, t_3 und u_3, ... und wir wollen jetzt den strengen Beweis führen, dass dieselben sämmtlich der Gleichung $t^2-Du^2=m^2$ Genüge leisten und dass ausser ihnen keine anderen ganzzahligen Lösungen möglich sind.

Zunächst folgt aus den angenommenen Gleichungen:

$$t_e+u_e\sqrt{D}=m\left(\frac{T}{m}+\frac{U\sqrt{D}}{m}\right)^e,\quad t_e-u_e\sqrt{D}=m\left(\frac{T}{m}-\frac{U\sqrt{D}}{m}\right)^e,$$

woher durch Multiplication

$$t_e^2-Du_e^2=m^2\left(\frac{T^2}{m^2}-\frac{DU^2}{m^2}\right)^e.$$

Da nun die Grösse in der Klammer rechts sich der Voraussetzung gemäss auf 1 reducirt, so wird der Werth der ganzen rechten Seite gleich 1, d. h. mit anderen Worten: das Werthsystem $t=t_e$ und $u=u_e$ befriedigt die vorgelegte Gleichung.

Dass dieses Werthsystem immer ganzzahlig sei, beweist man auf folgende Art. Es fällt nicht schwer die beiden Gleichungen

$$t_{e+1}+t_{e-1}=\frac{2T}{m}t_e,\quad u_{e+1}+u_{e-1}=\frac{2T}{m}u_e$$

zu verificiren. Der darin vorkommende Coefficient $\frac{2T}{m}$ stellt nun immer eine ganze Zahl dar. Denn da man $4T^2-4DU^2=m^2$ hat und $4D=4b'^2+4aa'$ durch m^2 ohne Rest theilbar ist (denn m ist der Voraussetzung zu Folge der grösste gemeinschaftliche Theiler zwischen a, $2b$, a'), so kann die linke Seite nur so durch m^2 theilbar sein, dass man $4T^2$ durch m^2 oder $2T$ durch m theilbar hat. Dies vorausgesetzt zeigen die vorstehenden Gleichungen unmittelbar, dass, wenn t_{e-1} und t_e, sowie u_{e-1} und u_e ganze Zahlen darstellen, eben dieses auch von den Zahlenausdrücken t_{e+1} und u_{e+1} behauptet werden kann. Nun ist dies der Fall für t_0, t_1 und u_0, u_1 also sind t_2 und e_2 ganze Zahlen; weil jetzt t_1, t_2, u_1, u_2 ganze Zahlen sind, sind es auch t_3, u_3 und indem man so weiter schliesst, ergiebt sich allgemein, dass die Ausdrücke t_e und u_e ganze Zahlen vorstellen. Zugleich erkennt man, dass sie mit wachsenden Indices gleichfalls wachsen und zwar bis ins Unendliche hinein. Nämlich aus der Gleichung $T^2-DU^2=m^2$ folgt $T>m$, also $\frac{2T}{m}\geqq 2$; diese Ungleichung auf unsere Reductionsformeln angewandt, giebt die beiden Ungleichungen $t_{e+1}>2t_e$, $u_{e+1}>2u_e$ (von denen die letzte jedoch in dem speciellen Falle $e=1$ möglicher Weise in die Gleichung $u_{e+1}=2u_e$ übergehen kann). Die Zahlen t, t_1, t_2, t_3, ... und u, u_1, u_2, u_3, ... wachsen daher in einem stärkeren Verhältnisse, als die Glieder einer geometrischen Progression, deren Exponent 2 ist; sie müssen daher gleich diesen beständig und bis ins Unendliche hinein wachsen.

Wir haben noch zum Schlusse den Beweis zu führen, dass die verschiedenen Zahlenwerthe, deren die Ausdrücke t_e und u_e fähig sind, alle nur möglichen Lösungssysteme unserer Gleichung enthalten.

Nehmen wir an, es existirte noch ein positives von allen diesen verschiedenes Lösungssystem, nämlich $t=t'$ und $u=u'$, so muss u', da die Zahlen u_e mit dem Index e von 0 bis ins Unendliche hinein wachsen, nothwendig zwischen irgend zwei benachbarten Werthen von u_e liegen, so dass man die Ungleichung

$$u_n < u' < u_{n+1}$$

setzen darf.

Um das Widersprechende in dieser Annahme herauszustellen, bemerken wir, dass sie die Existenz eines zweiten Lösungssystemes, nämlich

$$\tau = \frac{1}{m}(t't_n - Du'u_n), \quad v = \frac{1}{m}(u't_n - t'u_n)$$

nach sich zieht, und werden nachweisen, dass der Werth von v in diesem Lösungssysteme sowohl von 0, wie auch von U, welches der kleinsten positiven Lösung unserer Gleichung entspricht, verschieden ausfällt und mithin nothwendig der Ungleichung $v > U$ genügt.

Zunächst überzeugt man sich ohne Schwierigkeit durch directe Einsetzung des problematischen Lösungssystemes in die Gleichung $t^2 - Du^2 = m^2$, dass dieselbe befriedigt wird. Dass das System auch ganzzahlig ist, erhellt auf folgende Art. Die Gleichung $b^2 - D = -aa'$ hat, wenn man sie nach einander mit u'^2 und u_n^2 multiplicirt und die Gleichungen $t'^2 - Du'^2 = m^2$ und $t_n^2 - Du_n^2 = m^2$ berücksichtigt, die beiden Gleichungen zu Folge:

$$(bu'+t')(bu'-t') = -aa'u'^2 - m^2, \quad (bu_n + t_n)(bu_n - t_n) = -aa'u_n^2 - m^2.$$

Da die rechten Seiten dieser Gleichungen durch m^2 ohne Rest theilbar sind, so müssen es auch die linken sein. Nehmen wir zuerst speciell die erste Gleichung vor und bezeichnen die kleinsten positiven Reste, welche bei der Division von $bu'+t'$ und $bu'-t'$ durch m respective bleiben, mit r und ϱ, so hat man hiernach nothwendig $r\varrho$ als ein Multiplum von m^2 oder $r\varrho = lm^2$. Nun ist ferner $(bu'+t')+(bu'-t')$ ein Multiplum von m, weil m in $2b$ nach der Voraussetzung aufgeht, und $(bu'+t')-(bu'-t')$ gleichfalls ein solches Multiplum, weil, wie leicht erweislich, $2t'$ durch m ohne Rest getheilt werden kann: also hat man gemäss der Bedeutung von r und ϱ die Gleichungen $r+\varrho = hm$, $r-\varrho = km$. Der ersten dieser 3 Gleichungen, welche r und ϱ erhalten, kann man nun die Form $\frac{(r+\varrho)^2 - (r-\varrho)^2}{4} = lm^2$ geben und wendet man darauf die beiden letzten an, so erhalten wir $\frac{h^2 - k^2}{4} = lm^2$. Dies setzt voraus, dass die Zahlen h und k beide gleichzeitig entweder gerade oder ungerade sind; in beiden Fällen aber sind $h+k$ und $h-k$ gerade Zahlen. Wenden wir diese Bemerkung auf die mit Leichtigkeit herleitbaren Gleichun-

gen $2r = (h+k)m$ und $2\varrho = (h-k)m$ an, so kann man diese letzteren auf die Form $r = \frac{h+k}{2}m$, $\varrho = \frac{h-k}{2}.m$ bringen, aus welcher die Theilbarkeit von r und ϱ durch m hervorgeht oder mit anderen Worten, da r und ϱ Reste bezeichnen, die bei der Division mit m hervorgehen, hat man $r = 0$, $\varrho = 0$. Also sind die Ausdrücke $\frac{bu'+t'}{m}$ und $\frac{bu'-t'}{m}$ ganze Zahlen und eben dasselbe lässt sich in ähnlicher Weise von den Ausdrücken $\frac{bu_n+t_n}{m}$ und $\frac{bu_n-t_n}{m}$ darthun. Betrachtet man jetzt die Identität

$$u'(bu_n+t_n) - u_n(bu'+t') = u't_n - u_nt',$$

so sieht man augenblicklich ein, dass der Ausdruck $\frac{1}{m}(u't_n - u_nt')$, d. h. v eine ganze Zahl sei und, weil τ seine Bestimmung vermöge der Gleichung $\tau^2 - Dv^2 = m^2$ hat, so ist es gleichfalls eine ganze Zahl.

Der Zahlenwerth von v kann ferner weder gleich 0 sein, noch gleich U. Wäre $v = 0$, so folgte $u't_n = t'u_n$, $u'^2t_n^2 = t'^2u_n^2$ oder $u'^2(Du_n^2+m^2) = u_n^2(Du'^2+m^2)$, woher im Widerspruch zu der Annahme $u' = u_n$. Wäre v gleich U, so würde man, gleichfalls der Annahme widersprechend, $u_{n+1} = u'$, $t_{n+1} = t'$ erhalten. Es bestehen nämlich, wie man sich leicht durch Substitution der Ausdrücke für t_n, t_{n+1}, u_n, u_{n+1} überzeugen kann, die Identitäten:

$$u_{n+1}t_n - t_{n+1}u_n = mU,$$
$$t_{n+1}t_n - Du_{n+1}u_n = mT$$

und es ist daher, zu Folge der Werthe von v und τ, wenn wir $v = U$, $\tau = T$ annehmen: $u't_n - t'u_n = u_{n+1}t_n - t_{n+1}u_n$ und $t't_n - Du'u_n = t_{n+1}t_n - Du_{n+1}u_n$. Eliminiren wir aus diesen beiden Gleichungen t', so folgt $u'(t_n^2 - Du_n^2) = u_{n+1}(t_n^2 - Du_n^2)$, oder $u' = u_{n+1}$ im Widerspruche zur Annahme.

Also ist v eine ganze Zahl, die, wenn anders die Annahme Geltung hat, der vorgelegten Gleichung Genüge leistet und grösser als U ist, d. h. man hat $mv > mU$. Daraus folgt, wenn man für mv und mU ihre Werthe substituirt, die Ungleichung

$$u't_n - t'u_n > u_{n+1}t_n - t_{n+1}u_n.$$

Man ziehe jetzt aus den Gleichungen $t'^2 - Du'^2 = m^2$ und $t_{n+1}^2 - Du_{n+1}^2 = m^2$ die Werthe $\frac{t'}{u'} = \sqrt{D + \frac{m^2}{u'^2}}$ und $\frac{t_{n+1}}{u_{n+1}} = \sqrt{D + \frac{m^2}{u_{n+1}^2}}$; aus

ihnen ergiebt sich, da wir die hypothetische Ungleichung $u' < u_{n+1}$ haben, $\frac{t'}{u'} < \frac{t_{n+1}}{u_{n+1}}$ und dies hat die Ungleichung zu Folge:

$$t_n + u_n \frac{t'}{u'} > t_n + u_n \frac{t_{n+1}}{u_{n+1}}.$$

Multiplicirt man dieselbe mit der am Ende des vorigen Absatzes gefundenen, so erhält man

$$(u't_n - t'u_n)\left(t_n + u_n \frac{t'}{u'}\right) > (u_{n+1}t_n - t_{n+1}u_n)\left(t_n + u_n \frac{t_{n+1}}{u_{n+1}}\right)$$

oder, wenn man die Multiplication ausführt, wobei die mittleren Glieder sich rechts und links gegen einander aufheben:

$$u't_n^2 - \frac{u_n^2 t'^2}{u'} > u_{n+1}t_n^2 - \frac{u_n^2 t_{n+1}^2}{u_{n+1}}.$$

Substituiren wir hier für t_n^2, t_{n+1}^2, t'^2 ihre Werthe $m^2 + Du_n^2$, $m^2 + Du_{n+1}^2$, $m^2 + Du'^2$, so erhält man nach einigen leichten Reductionen:

$$\frac{m^2u'^2 - m^2u_n^2 + Du'^2u_n^2(m^2-1)}{u'} > \frac{m^2u_{n+1}^2 - m^2u_n^2 + Du_{n+1}^2u_n^2(m^2-1)}{u_{n+1}},$$

woher nach Multiplication mit $u'u_{n+1}$ und Zusammenziehung:

$$\left\{m^2u'u_{n+1} + m^2u_n^2 + Du'u_{n+1}u_n^2(m^2-1)\right\}\left\{u' - u_{n+1}\right\} > 0.$$

Nun ist, da m niemals der 0 gleich sein kann, die Grösse in der ersten Doppelklammer links stets positiv; damit also ihr Product mit der zweiten Doppelklammer positiv ausfalle, ist nothwendig, dass $u' - u_{n+1}$ gleichfalls positiv sei, d. h. dass man gegen die Voraussetzung $u' > u_{n+1}$ habe.

Also giebt es ausser den Werthen, deren die Zahlenausdrücke t_s und u_s fähig sind, keine anderen Lösungssysteme der Gleichung $t^2 - Du^2 = m^2$.

4) Auflösung der Geichung $Ax^2 + 2Bxy + Cy^2 = M$ in relativen Primzahlen für x, y, wenn die Determinante D positiv und nicht quadratisch ist.

Sei irgend eine Lösung der Hülfsgleichung $z^2 - D = Ms$ in den kleinsten Zahlen dargestellt durch $z = \zeta$, $s = \sigma$, so handelt es sich darum, alle nur möglichen Repräsentationen von M durch (A, B, C) zu finden, welche dieser Lösung der Hülfsgleichung zugehören oder liirt sind. Denn die Untersuchung der übrigen Lösungen wird ganz in gleicher Weise vor sich gehen, und, wenn solche vorhanden sind, alle übrig gebliebenen Repräsentationen liefern. Nehmen wir also an, die Form (A, B, C) habe sich als aequivalent ausgewiesen mit der Form (M, ζ, σ), d. h. es exi-

stiren solche Repräsentationen von M, die zu der Lösung ζ, σ gehören. Dies vorausgesetzt ist schon früher gezeigt, dass eine Transformation von (A, B, C) in (M, ζ, σ) immer bestimmt werden könne: sei dieselbe vorgestellt durch die Substitutionsformeln $x = \alpha\xi + \beta\eta$, $y = \gamma\xi + \delta\eta$ und werde durch t, u in allgemeinster Weise ein Lösungssystem der Gleichung $t^2 - Du^2 = m^2$ bezeichnet, wo D und m die bekannte Bedeutung haben, so hat man folgende Formeln, unter denen alle (eigentlichen) Transformationen von (A, B, C) in (M, ζ, σ) enthalten sind:

$$x = \frac{1}{m}\Big\{\alpha t - (B\alpha + C\gamma)u\Big\}\xi + \frac{1}{m}\Big\{\beta t - (B\gamma + C\delta)u\Big\}\eta,$$

$$y = \frac{1}{m}\Big\{\gamma t + (A\alpha + B\gamma)u\Big\}\xi + \frac{1}{m}\Big\{\delta t + (A\beta + B\delta)u\Big\}\eta$$

und die sämmtlichen der Lösung ζ, σ liirten Repräsentationen von M durch (A, B, C) stehen unter der allgemeinen Form:

$$x = \frac{1}{m}\Big\{\alpha t - (B\alpha + C\gamma)u\Big\},$$

$$y = \frac{1}{m}\Big\{\gamma t + (A\alpha + B\gamma)u\Big\}.$$

Wenden wir das Gesagte auf die in §. 24. am Schlusse behandelte Gleichung

$$4x^2 + 28xy + 20y^2 = 956$$

an, so hatte die Hülfsgleichung 4 verschiedene Lösungen, von denen sich indessen nur zwei brauchbar zeigten, nämlich

$$\zeta = 366,\ \sigma = 140 \text{ und } \zeta = -366,\ \sigma = 140.$$

Wir hatten demgemäss eine Transformation von (4, 14, 20) gesucht in jede der beiden Formen (956, 366, 140) und (956, —366, 140). Dieselben waren respective:

$$x = -3\xi - \eta,\ y = -5\xi - 3\eta,$$

$$x = -27\xi + 10\eta,\ y = 35\xi - 13\eta,$$

also haben wir im ersten Falle $\alpha = -3$, $\gamma = -5$, im zweiten $\alpha = -27$, $\gamma = 35$ und in beiden Fällen gemeinschaftlich $m = 4$, $A = 4$, $B = 14$, $C = 20$. Indem wir diese Werthe in die so eben aufgestellten allgemeinen Repräsentationsformeln einsetzen und die gehörigen Reductionen vornehmen, bekommen wir die beiden einzig möglichen Systeme von Repräsentationen:

$$x = -\frac{3}{4}t + \frac{71}{2}u, \quad y = -\frac{5}{4}t - \frac{41}{2}u;$$

$$x = -\frac{27}{4}t - \frac{161}{2}u, \quad y = -\frac{35}{4}t + \frac{191}{2}u,$$

und die in diesen Formeln auftretenden Hülfsgrössen t und u müssen der Gleichung

$$t^2 - 116u^2 = 16$$

Genüge leisten. Dass dieses der Fall sein muss, kann man mit Leichtigkeit verificiren. Setzt man nämlich beide Repräsentationssysteme in unsere vorgegebene Gleichung ein, so erhält man nach einigen leichten Reductionen respective

$$(3t - 142u)^2 + 7(3t - 142u)(5t + 82u) + 5(5t + 82u)^2 = 16 \,.\, 239,$$
$$(27t + 322u)^2 - 7(27t + 322u)(35t + 382u) + 5(35t + 382u)^2 = 16 \,.\, 239,$$

und beide Gleichungen reduciren sich nach Ausführung der Multiplication auf

$$239\,(t^2 - 116u^2) = 16 \,.\, 239.$$

Gehen wir jetzt zur Auflösung der Gleichung $t^2 - 116u^2 = 16$ über, so muss man sich eine reducirte Form bestimmen, wie $(a, b, -a')$, so dass der Coefficient a positiv und $m = 4$ der grösste gemeinschaftliche Theiler von a, $2b$, a' ist. Eine solche Form ist (cf. §. 24.) die Form $(4, 10, -4)$, also $a = 4$, $b = 10$, $a' = -4$. Man hat sich nun $\frac{\sqrt{D} - b}{a} = \frac{\sqrt{116} - 10}{4} = \frac{\sqrt{29} - 5}{2}$ in einen Kettenbruch zu verwandeln und findet sofort

$$\frac{\sqrt{29} - 5}{2} = \cfrac{1}{5 + \cfrac{1}{5 + \cfrac{1}{5 + \cfrac{1}{5 + \dots}}}}$$

also die Periode eingliedrig. Da 1 eine ungerade Zahl ist, sind mithin die beiden letzten Näherungswerthe, die zur doppelt genommenen Periode gehören, zu bestimmen, d. h. geradezu die beiden ersten, nämlich $\frac{1}{5}$ und $\frac{5}{26}$. Bedienen wir uns jetzt zur Berechnung der kleinsten Lösung der Formeln

$$T = \left(Z_{n-1} + \frac{b}{a'} Z_n\right) . m, \quad U = \frac{Z_n . m}{a},$$

so haben wir $Z_{n-1} = 1$, $Z_n = 5$ einzusetzen und bekommen $T = \left(1 + \frac{5}{2} . 5\right) . 4 = 54$, $U = \frac{5 \,.\, 4}{4} = 5$. Die allgemeinen Formeln für ein beliebiges Lösungssystem werden jetzt

$$t_e = 2\left(\frac{27+5\sqrt{29}}{2}\right)^e + 2\cdot\left(\frac{27-5\sqrt{29}}{2}\right)^e,$$

$$u_e = \frac{1}{\sqrt{29}}\left(\frac{27+5\sqrt{29}}{2}\right)^e - \frac{1}{\sqrt{29}}\left(\frac{27-5\sqrt{29}}{2}\right)^e.$$

Hieraus ergiebt sich, indem man für e der Reihe nach die Werthe 0, 1, 2, 3, ... einsetzt:

$$t_0 = 4,\ u_0 = 0,$$

$$t_1 = 4\cdot\frac{27}{2} = 54,\ u_1 = \frac{2}{\sqrt{29}}\cdot\frac{5\sqrt{29}}{2} = 5,$$

$$t_2 = 4\cdot\frac{27^2+25\cdot29}{4} = 1454,\ u_2 = \frac{2}{\sqrt{29}}\cdot\frac{10\cdot27\sqrt{29}}{4} = 135,$$

$$t_3 = 4\cdot\frac{27^3+81\cdot25\cdot29}{8} = 39204,\ u_3 = \frac{2}{\sqrt{29}}\cdot\frac{27^2\cdot15\sqrt{29}+5^3\cdot29\sqrt{29}}{8} = 3640,$$

. . . .

. . . .

Substituiren wir endlich diese Werthe in unsere beiden Systemen allgemeinen Repräsentationsformeln, so bekommen wir nach einander:

$$x_0 = -\frac{3}{4}\cdot4 \pm \frac{71}{2}\cdot0 = -4,\ y = -\frac{5}{4}\cdot4 \mp \frac{41}{2}\cdot0 = -5,$$

$$x_1 = -\frac{3}{4}\cdot54 \pm \frac{71}{2}\cdot5 = \begin{cases}+137\\-218\end{cases},\ y_1 = -\frac{5}{4}\cdot54 \mp \frac{41}{2}\cdot5 = \begin{cases}-170\\+\ 35\end{cases},$$

$$x_2 = -\frac{3}{4}\cdot1454 \pm \frac{71}{2}\cdot135 = \begin{cases}+3702\\-5883\end{cases},\ y_2 = -\frac{5}{4}\cdot1454 \mp \frac{41}{2}\cdot135 = \begin{cases}-4585\\+\ 950\end{cases}.$$

. . . .

. . . .

$$x_0 = -\frac{27}{4}\cdot4 \mp \frac{161}{2}\cdot0 = -27,\ y_0 = \frac{35}{4}\cdot4 \pm \frac{191}{2}\cdot0 = 35,$$

$$x_1 = -\frac{27}{4}\cdot54 \mp \frac{161}{2}\cdot5 = \begin{cases}-767\\+\ 38\end{cases},\ y_1 = \frac{35}{4}\cdot54 \pm \frac{191}{2}\cdot5 = \begin{cases}+950\\-\ 5\end{cases},$$

$$x_2 = -\frac{27}{4}\cdot1454 \mp \frac{161}{2}\cdot135 = \begin{cases}-20682\\+\ 1053\end{cases},\ y_2 = \frac{35}{4}\cdot1454 \pm \frac{191}{2}\cdot135 = \begin{cases}+25615\\-\ 170\end{cases}$$

. . . .

. . . .

Betrachten wir die Repräsentationen, welche durch die zweite Lösungsreihe erhalten werden, so ist offenbar die einfachste unter ihnen $x = +38$, $y = -5$ und unser zweites System von Repräsentationsformeln daher einer einfacheren Gestalt fähig. Zu dem Zwecke hat man

nur nöthig, indem A, B, C, m ihre früheren Werthe 4, 14, 20, 4 beibehalten, in die allgemeinen Repräsentationsformeln $\alpha = +38$, $\gamma = -5$ einzuführen; dadurch gehen dieselben über in:

$$x = \frac{19}{2}t - 108u,\ y = -\frac{5}{4}t + \frac{41}{2}u$$

und man bekommt für die verschiedenen Werthe von t und u folgende Resultate:

$$x_0 = \frac{19}{2}.4 \mp 108.0 = 38,\ y_0 = -\frac{5}{4}.4 \pm \frac{41}{2}.0 = -5;$$

$$x_1 = \frac{19}{2}.54 \mp 108.5 = \begin{cases} -27 \\ +1053 \end{cases},\ y_1 = -\frac{5}{4}.54 \pm \frac{41}{2}.5 = \begin{cases} +35 \\ -170 \end{cases};$$

$$x_2 = \frac{19}{2}.1454 \mp 108.135 = \begin{cases} -767 \\ +28393 \end{cases},\ y_2 = -\frac{5}{4}.1454 \pm \frac{41}{2}.135 = \begin{cases} +950 \\ -4585 \end{cases}.$$

. . . .

. . . .

Die gewonnenen Resultate stimmen vollständig mit denen überein, die die Rechnung mit dem nämlichen Beispiele am Schlusse des §. 24. gehabt hat.

Zu einer vollständigen Lösung unserer Gleichung $4x^2 + 28xy + 20y^2 = 956$ gehören aber auch diejenigen Lösungen nach x und y, die nicht relative Primzahlen zu einander sind; dieselben werden erhalten, da 956 nur den einzigen quadratischen Factor 4 enthält, wenn man $x = 2x'$, $y = 2y'$ setzt und die Gleichung

$$4x'^2 + 28x'y' + 20y'^2 = 239$$

auflöst. Dieselbe ist aber nicht möglich (wenigstens nicht für ganzzahlige Werthe von x und y), weil 239 nicht durch 4 getheilt werden kann; also hat unsere vorgelegte Gleichung überhaupt keine Lösungen, als solche, die relative Primzahlen zu einander sind.

Beispiel 2. Die vorgelegte Gleichung sei

$$x^2 - 48y^2 = 39^2 = 1521,$$

also $D = 48$, $m = 1$. Die Hülfsgleichung ist $z^2 - 48 = 1521s$ oder $z^2 \equiv 48 \pmod{9.13^2}$. Nun ist 48 nach dem Modul 9 der Zahl 3 congruent, also ein Nichtrest von 9 und demzufolge auch von 1521. Mithin ist die Bedingungscongruenz unmöglich und gemäss dem Fundamentaltheoreme pag. 318 keine Lösung der vorgelegten Gleichung in relativen Primzahlen für x und y möglich. Wenn nun solche Lösungen existiren,

die keine relativen Primzahlen enthalten, so können sie, da 1521 nur 3 von einander verschiedene quadratische Factoren hat (unter denen die 1 nicht mit zählt), nur von einer der Formen $x = 39x'$ und $y = 39y'$, $x = 13x'$ und $y = 13y'$, $x = 3x'$ und $y = 3y'$ sein; dem entsprechend sind die drei Gleichungen $x'^2 - 48y'^2 = 1$, $x'^2 - 48y'^2 = 9$, $x'^2 - 48y'^2 = 169$ in relativen Primzahlen für x' und y' aufzulösen. Von denselben ist die mittlere wieder nicht möglich (wenigstens in relativen Primzahlen für x, y), weil 48 ein Nichtrest von 9 ist; also sind nur die erste und dritte Gleichung zu betrachten.

a) Die Gleichung $x'^2 - 48y'^2 = 1$ geht für $x' = t$, $y' = u$ geradezu über in die Gleichung $t^2 - 48u^2 = 1$ und wir müssen uns daher eine reducirte Form mit positivem ersten Coefficienten suchen, deren Determinante 48 ist und deren Coefficienten 1 zum grössten gemeinschaftlichen Maasse haben. Eine solche Form ist unter anderen $(a, b, -a') = (1, 6, -12)$ und man findet jetzt durch Verwandlung von $\frac{\sqrt{D} - b}{a} = \sqrt{48} - 6$ in einen Kettenbruch

$$\sqrt{48} - 6 = \frac{1}{1} + \frac{1}{12} + \frac{1}{1} + \frac{1}{12} + \ldots;$$

also hat die Periode eine gerade Anzahl von Gliedern, nämlich zwei. Die beiden ersten Näherungswerthe sind $\frac{1}{1}$ und $\frac{12}{13}$ und man findet als die kleinste Lösung unserer Gleichung $T = 7$, $U = 1$. Daraus folgen die allgemeinen Lösungsformeln

$$x' = t_e = \frac{1}{2}(7 + 4\sqrt{3})^e + \frac{1}{2}(7 - 4\sqrt{3})^e;$$

$$y' = u_e = \frac{1}{8\sqrt{3}}(7 + 4\sqrt{3})^e - \frac{1}{8\sqrt{3}}(7 - 4\sqrt{3})^e,$$

aus dem unter anderen folgende partikulären fliessen:

$$x' = t_0 = 1,\ y' = u_0 = 0;\ x' = t_1 = 97,\ y' = u_1 = 14;$$
$$x' = t_2 = 1351,\ y' = u_2 = 195.$$

. . . .

. . . .

Die Berechnung dieser verschiedenen Zahlenwerthe wird am einfachsten mit Hülfe der Recursionsformeln

$$t_{e+1} = \frac{2T}{m} t_e - t_{e-1}, \quad u_{e+1} = \frac{2T}{m} u_e - u_{e-1}$$

ausgeführt werden.

b) Was die zweite Gleichung $x'^2 - 48y'^2 = 169$ anbetrifft, so hat die Hülfsgleichung $z^2 - 48 = 169s$ nur zwei von einander verschiedene Lösungen, nämlich $z = \pm 75$, $s = 33$; wir haben daher die Form $(1, 0, -48)$ zu vergleichen mit den beiden Formen $(169, 75, 33)$ und $(169, -75, 33)$; zugleich wissen wir, da die erste zweideutig ist, dass dieselbe entweder beiden zugleich eigentlich (und auch uneigentlich) äquivalent ist, oder keiner von beiden, d. h. wenn die eine irgend welchen Repräsentationen liirt ist, so ist es auch die andere. Die Aufsuchung der reducirten Formen giebt folgende Reihe von angrenzenden Formen:

$$(1, 0, -48), (-48, 48, -47), (-47, 46, -44), (-44, 42, -39),$$
$$(-39, 36, -32), (-32, 28, -23), (-23, 18, -12), (-12, 6, 1),$$
$$(1, 6, -12);$$

$$(169, \; 75, 33), (33, -9, 1), (1, \; 6, -12);$$
$$(169, -75, 33), (33, \; 9, 1), (1, -6, -12).$$

Die erste und zweite, sowie die erste und dritte dieser Formenreihen setzen sich nun respective, wie folgt, zu einer einzigen zusammen:

$$(1, 0, -48), (-48, 48, -47), (-47, 46, -44), (-44, 42, -39),$$
$$(-39, 36, -32), (-32, 28, -23), (-23, 18, -12), (-12, 6, 1),$$
$$(1, 9, 33), (33, -75, 169), (169, 75, 33)$$

und

$$(1, 0, -48), (-48, 48, -47), (-47, 46, -44), (-44, 42, -39),$$
$$(-39, 36, -32), (-32, 28, -23), (-23, 18, -12), (-12, -6, 1),$$
$$(1, -9, 33), (33, 75, 169), (169, -75, 33).$$

Hieran knüpft sich folgende weitere Rechnung:

	-1	-2	-2	-2	-2	-2	-2	15	-2	0
$\frac{0}{1}$	$\frac{-1}{-1}$	$\frac{2}{1}$	$\frac{-3}{-1}$	$\frac{4}{1}$	$\frac{-5}{-1}$	$\frac{6}{1}$	$\frac{-7}{-1}$	$\frac{-111}{-16}$	$\frac{229}{33}$	$\frac{111}{16}$
							-1	-15	2	0
							$\frac{-1}{0}$	$\frac{9}{-1}$	$\frac{19}{-2}$	$\frac{21}{1}$

Hiernach hat man folgende beiden partikulären Repräsentationen :

$$x' = \alpha = 229,\quad y' = \gamma = 33,$$
$$x' = \alpha = 19,\quad y' = \gamma = -2,$$

welche zu entgegengesetzten Lösungen unserer Hülfsgleichung gehören, und es folgen daraus die beiden allgemeinen Systeme von Repräsentationen

$$x' = 229t \pm 1584u,\quad y' = 33t \pm 229u;$$
$$x' = 19t \mp 96u,\quad y' = -2t \pm 19u,$$

von denen keines irgend eine Repräsentation des anderen enthalten kann. Die Zahlen t und u in diesen Formeln bestimmen sich vermöge der Gleichung $t^2 - 48u^2 = 1$ und sind mit den unter a) soeben vorgekommenen Grössen t_e und u_e identisch. Was das erste System anbetrifft, so gestattet es eine einfachere Form, weil ein einfacheres Lösungssystem als das zu seiner Bildung benutzte existirt. Dasselbe ist $x' = \alpha = 37$ und $y' = \gamma = -5$ und wird erhalten, wenn man in dem genannten Systeme für t und u die Werthe 97 und 14 einsetzt und nur das andere Vorzeichen berücksichtigt. Benutzen wir dieses Lösungssystem, so bekommen wir für unser erstes System von Repräsentationen die einfachere Gestalt

$$x' = 37t - 240u,\quad y' = -5t + 37u.$$

Das Resultat aus unserer gesammten Rechnung ist, dass, wenn man unter e eine beliebige ganze positive Zahl versteht (die 0 als solche mit gerechnet), jede Repräsentation von 1521 durch die Form (1, 0, —48) nothwendig enthalten ist unter einem der folgenden Systeme von Formeln:

$$\text{I.}\quad \begin{cases} \dfrac{x}{39} = t = \tfrac{1}{2}(7+4\sqrt{3})^e + \tfrac{1}{2}(7-4\sqrt{3})^e, \\[2mm] \dfrac{y}{39} = u = \dfrac{1}{8\sqrt{3}}(7+4\sqrt{3})^e - \dfrac{1}{8\sqrt{3}}(7-4\sqrt{3})^e; \end{cases}$$

$$\text{II.}\quad \frac{x}{3} = 37t \mp 240u,\quad \frac{y}{3} = -5t \pm 37u;$$

$$\text{III.}\quad \frac{x}{3} = 19t \mp 96u,\quad \frac{y}{3} = -2t \pm 19u.$$

Beispiel 3. Sei die vorgelegte Gleichung

$$42x^2 + 62xy + 21y^2 = 585,\quad D = 79,\quad m = 1;$$

alsdann findet man in relativen Primzahlen folgende Lösungssysteme für x und y:

$$x = 3t - 114u,\quad y = t + 157u;$$
$$x = 63t - 746u,\quad y = -67t + 789u,$$

und in solchen Zahlenwerthen von x und y, die den gemeinschaftlichen Factor 3 haben, gleichfalls zwei, nämlich:

$$x = 6t - 123u,\ y = -3t + 159u;$$
$$x = 66t - 597u,\ y = -69t + 633u.$$

Ausser diesen vier Lösungssystemen giebt es weiter keine und die Zahlen t und u, die hier vorkommen, bezeichnen alle nur möglichen Zahlenwerthe, welche der Gleichung

$$t^2 - 79u^2 = 1$$

Genüge leisten. Setzen wir der Einfachheit halber fest, dass t und u blos positive Zahlenwerthe sein sollen, die die genannte Eigenschaft besitzen, so wird man durch Variation der Vorzeichen aus jedem der vier obigen Formelsysteme sich vier verschiedene Lösungssysteme ziehen können. So z. B. folgen aus dem ersten Formelsysteme folgende vier:

$$x = 3t - 114u,\ y = t + 157u;$$
$$x = 3t + 114u,\ y = t - 157u;$$
$$x = -3t - 114u,\ y = -t + 157u;$$
$$x = -3t + 114u,\ y = -t - 157u.$$

5) Verschiedene Bemerkungen die Gleichung $t^2 - Du^2 = m^2$ betreffend (D positiv).

a) Die Gleichung $t^2 - Du^2 = m^2$ ist immer vermöge der partikulären unter 3) auseinander gesetzten Methode auflösbar, wenn eine Form $(a, b, -a')$ existirt, deren Determinante gleich D ist und deren Coefficienten a, $2b$, a' zum grössten gemeinschaftlichen Theiler haben. Denn entweder ist diese Form eine reducirte, oder sie führt die Existenz wenigstens einer reducirten Form herbei, welche diese Eigenschaften hat (streng genommen sogar von mindestens zwei solchen Formen; denn die Periode jeder reducirten Form enthält eine gerade Anzahl von Formen, also wenigstens zwei; unter diesen ist mindestens immer eine, deren erster Coefficient eine positive Grösse ist). Hierzu wird es nicht überflüssig sein, die Bemerkung zu machen, dass, wenn eine solche Form $(a, b, -a')$ nicht existiren sollte, daraus durchaus nicht ohne Weiteres die Unmöglichkeit der genannten Gleichung gefolgert werden darf. Vielmehr ist eine solche Gleichung dann nach den allgemeinen Principien zu behandeln, d. h. es ist zu untersuchen, ob und wie viele Repräsentationen von m^2 durch die Form $(1, 0, -D)$ möglich seien. Ein Beispiel hierzu giebt

das zweite der vorigen Nummer; die dort behandelte Gleichung kommt für $x = t$ und $y = u$ auf die Form $t^2 - 48u^2 = 1521$ und offenbar kann keine auf die Determinante 48 bezügliche reducirte Form der verlangten Art existiren — und gleichwohl hat sich die Gleichung als eine mögliche herausgestellt. Schliesslich freilich wird die allgemeine Methode immer auf eine Gleichung von der Form $t^2 - Du^2 = m^2$ führen, welche unmittelbar zu Folge der Umstände, vermöge deren sie erhalten wird, unsere specielle Auflösungsmethode nicht blos gestattet, sondern auch fordert.

Bei dieser Sachlage ist es nicht überflüssig die Relationen aufzusuchen, welche zwischen D und m eintreten müssen, damit die specielle Auflösungsmethode anwendbar sei. Bezeichnen wir zu dem Zwecke den grössten quadratischen Theiler (der unter Umständen auch gleich 1 sein kann) der Determinante D mit n^2, so wird, wenn man $D = n^2D'$ setzt, D' keinen quadratischen Factor mehr enthalten können.

Nehmen wir jetzt zuerst an, D' habe die Form $4k + 1$: dann wird, vermöge unserer speciellen Auflösungsmethode, die Gleichung $t^2 - Du^2 = m^2$ für alle solche Werthe von m aufgelöst werden können, welche Divisoren von $2n$ sind, und umgekehrt, wenn sie vermöge unserer speciellen Methode in ganzen Zahlen für t und u gelöst werden kann für irgend einen besonderen Werth von m (d. h. wenn eine Form $(a, b, -a')$ existirt, deren Determinante D ist und deren Coefficienten a, $2b$, a' zum grössten gemeinschaftlichen Masse die Zahl m haben), so ist m ein Divisor von $2n$.

Der erste Theil unserer Behauptung erhellt sofort aus der Betrachtung der Form $\left(m, n, -\frac{n^2(D'-1)}{m}\right)$. Dieselbe hat nämlich die Determinante D und die Zahl m ist der grösste gemeinschaftliche Theiler der Coefficienten m, $2n$, $-\frac{n^2(D'-1)}{m}$. Um das letzte darzuthun ist nur nöthig zu zeigen, dass der Ausdruck $\frac{n^2(D'-1)}{m^2}$ eine ganze Zahl ist. Dies erhellt aber leicht, wenn man ihn auf die Form $\left(\frac{2n}{m}\right)^2 \cdot \frac{D'-1}{4}$ bringt; denn alsdann ist jeder Factor eine ganze Zahl, der erste, weil $2n$ als durch m theilbar und der letzte, weil D' als von der Form $4k + 1$ vorausgesetzt wird. — Die Umkehrung folgt ebenso leicht. Da m der grösste

gemeinschaftliche Theiler zwischen den Coefficienten a, $2b$, a' einer existirenden reducirten Form ist, so ist m^2 ein Theiler von $4D = 4b^2 + 4aa'$, also auch von $4n^2 D'$. Daraus folgt aber, dass m die Zahl $2n$ misst. Denn wäre dieses nicht der Fall, so müsste der grösste gemeinschaftliche Divisor zwischen $2n$ und m kleiner als m sein, etwa gleich δ und indem man unter m' und n' relative Primzahlen zu einander versteht, die beide grösser als 1 sind, würde folgen $m' = m'\delta$, $2n = n'\delta$; mithin könnte $4n^2.D'$ nur so durch m^2 theilbar sein, dass man m'^2 als einen Theiler von D' hätte: dies ist aber gegen die Voraussetzung, dass D' keinen von 1 verschiedenen quadratischen Factor enthält.

Nehmen wir zweitens an, D' sei von einer der beiden Formen $4k+2$ oder $4k+3$: dann wird, vermöge unserer speciellen Auflösungsmethode, die Gleichung $t^2 - Du^2 = m^2$ für alle solche Werthe von m aufgelöst werden können, welche Divisoren von n sind, und umgekehrt, wenn diese Auflösungsmethode für irgend einen besonderen Werth von m anwendbar ist, so muss m ein Divisor von n sein.

Der erste Theil des Satzes ergiebt sich durch Betrachtung der Form $\left(m, 0, -\frac{n^2 D'}{m}\right)$, welche einmal die Determinante D und dann auch ersichtlich m zum grössten gemeinschaftlichen Theiler ihrer Coefficienten hat. Umgekehrt, wenn eine Form $(a, b, -a')$ existirt, die m zum grössten gemeinschaftlichen Theiler hat, lässt sich beweisen, dass m ein Theiler von n sei. Zunächst folgt wieder m^2 als ein Theiler von $4D = 4b^2 + 4aa'$, also ist m^2 auch ein Theiler von $4n^2 D'$. Ganz in derselben Weise, wie im ersten Falle, leitet man hieraus her, dass $2n$ durch m getheilt werden kann. Hieraus würde folgen, dass n durch m theilbar ist, wenn der Quotient $\frac{2n}{m}$ eine gerade Zahl wäre. Um dieses zu zeigen, nehmen wir ihn als ungerade an; dann wäre $\left(\frac{2n}{m}\right)^2$, wie alle Quadrate ungerader Zahlen, von der Form $4k+1$, also $\frac{4n^2}{m^2} \equiv 1 \pmod 4$; demzufolge hat man, je nachdem D' von der Form $4k+2$ oder von der Form $4k+3$ ist, $\frac{4n^2 D'}{m^2} \equiv$ entweder 2 oder 3 $(mod\ 4)$. Nun ist aber

$$\frac{4n^2 D'}{m^2} = \frac{4D}{m^2} = \frac{4b^2 + 4aa'}{m^2} = \left(\frac{2b}{m}\right)^2 + 4\frac{aa'}{m^2}, \text{ also } \equiv \left(\frac{2b}{m}\right)^2 \pmod 4.$$

Dies in die vorige Congruenz eingesetzt, giebt $\left(\frac{2b}{m}\right)^2 \equiv$ entweder 2 oder 3 $(mod\ 4)$. Beides ist aber gleichmässig unstatthaft, da ebensowohl 2, wie 3 ein Nichtrest von 4 ist.

Aus der vorstehenden Analyse ergiebt sich unter Anderen, dass das unter dem Namen des Pell'schen bekannte Problem, die Gleichung $t^2 - Du^2 = 1$ in ganzen Zahlen für t und u aufzulösen, immer möglich ist; ferner folgt, dass die Gleichung $t^2 - Du^2 = 4$ immer auflösbar ist, sobald D eine der Formen $4k$ oder $4k+1$ hat; in allen anderen Fällen ist dieselbe wenigstens nicht vermöge der speciellen Methode, die wir hier ins Auge fassen, aufzulösen.

Wenn m grösser als 2 ist, aber eine Zahl, für welche diese Methode Anwendung findet, so kann man die Gleichung $D^2 - Du^2 = m^2$ immer auf eine ähnliche Gleichung zurückführen, in welcher m entweder den Werth 1 oder 2 hat. Untersuchen wir die beiden möglichen Fälle, indem m entweder schon ein Theiler von n sein kann, oder doch wenigstens ein Theiler von $2n$. Wenn m die Zahl n theilt, so ist m^2 ein Theiler von $D = n^2 D'$ und man löse sich daher die Gleichung $t'^2 - \frac{D}{m^2} u'^2 = 1$ auf; die Lösungen der vorgelegten Gleichung sind alsdann $t = mt'$, $u = u'$. — Wenn dagegen m wohl die Zahl $2n$, aber nicht die Zahl n theilt, so ist m nothwendig eine gerade Zahl, also $\frac{m}{2}$ ganz. Ferner ist m^2 ein Theiler von $4D$ (denn sei die reducirte Form, welche zur Auflösung der vorgelegten Gleichung tauglich ist, $(a,\ b,\ -a')$, so ist $4D = (2b)^2 + 4aa'$). Man löse daher die Gleichung $t'^2 - \frac{4D}{m^2} u'^2 = 4$ in ganzen Zahlen für t' und u' auf, so sind $t = \frac{m}{2} t'$ und $u = u'$ die Lösungen der vorgelegten Gleichung.

b) Wie wir wissen, sind die auf einander folgenden Lösungen der Gleichung $t^2 - Du^2 = m^2$, wie sie sich vermöge der Ausdrücke von t_e und u_e ergeben, durch die Recursionsformeln $t_{e+1} + t_{e-1} = \frac{2T}{m} t_e$ und $u_{e+1} + u_{e-1} = \frac{2T}{m} u_e$ mit einander verknüpft. Aus diesen beiden Relationen ergiebt sich eine bemerkenswerthe Eigenschaft der Zahlen t_e und u_e, von der wir weiter unten eine Anwendung machen werden. Indem wir näm-

lich irgend einen beliebigen Modul h uns annehmen, existirt immer eine Zahl k von der Beschaffenheit, dass die Zahlen

$$t_0,\ t_1,\ t_2,\ \ldots\ldots\ t_{k-1} \text{ und } u_0,\ u_1,\ u_2,\ \ldots\ldots\ u_{k-1},$$

nach dem Modul h der Reihe nach congruent werden den Zahlen

$$t_k,\ t_{k+1},\ t_{k+2},\ \ldots\ldots\ t_{2k-1} \text{ und } u_k,\ u_{k+1},\ u_{k+2},\ \ldots\ldots\ u_{2k-1}$$

und weiter den Zahlen

$$t_{2k},\ t_{2k+1},\ t_{3k+1},\ \ldots\ldots\ t_{4k-1} \text{ und } u_{2k},\ u_{2k+1},\ u_{2k+2},\ \ldots\ldots\ u_{3k-1}$$

und so weiter fort bis ins Unendliche. Mithin hat man allgemein die beiden Congruenzen $t_\mu \equiv t_\nu\ (mod\ h)$ und $u_\mu \equiv u_\nu\ (mod\ h)$, sobald zwischen den Indices die Congruenz $\mu \equiv \nu\ (mod\ k)$ besteht. Also die Zahlen t_0, t_1, ... t_{k-1} und ebenso die Zahlen u_0, u_1, u_2, ... u_{k-1} vertheilen sich nach irgend einem beliebigen Modul in eine endliche Menge von Gruppen, die eine unbegrenzte Menge von an den entsprechenden Stellen unter einander congruenten Zahlen enthalten. — Zunächst erhellt leicht, dass die behaupteten Congruenzen sämmtlich bestehen, sobald man die folgenden Congruenzen beweisen kann:

$$t_k \equiv t_0,\ t_{k+1} \equiv t_1,\ u_k \equiv u_0,\ u_{k+1} \equiv u_1\ (mod\ h).$$

Betrachten wir z. B. die Gleichung $t_{k+2} + t_k = \frac{2T}{m} t_{k+1}$, so geht dieselbe zu Folge der für den Augenblick vorausgesetzten Congruenzen über in die Congruenz $t_{k+2} + t_0 \equiv \frac{2T}{m} t_1\ (mod\ h)$ oder, da die Gleichung $t_2 + t_0 = \frac{2T}{m} t_1$ besteht, $t_{k+2} \equiv t_2\ (mod\ h)$; ebenso beweist man die Congruenz $u_{k+2} \equiv u_2\ (mod\ h)$ und die weiter folgenden Congruenzen $t_{k+3} \equiv t_3$, $u_{k+3} \equiv u_3$, u. s. w.

Um die genannten 4 Congruenzen, aus denen alle übrigen folgen, zu beweisen, bemerken wir zuerst, dass für jeden bestimmten Werth von h immer eine Zahl λ existirt, welche für k eingesetzt die dritte Congruenz befriedigt. Man löse sich zu dem Zweck die Hülfsgleichung $t'^2 - h^2 D u'^2 = m^2$ auf, was zu Folge der unter a) auseinander gesetzten Principien immer möglich ist (nämlich zu Folge der Voraussetzung ist $t^2 - Du^2 = m^2$ vermöge unserer partikulären Methode auflösbar, also, wenn man $D = n^2 D'$ setzt, m ein Theiler entweder von n oder von $2n$ und demzufolge auch entweder von hn oder von $2hn$). Sei die Lösung in den kleinsten Zahlen T', U': so ist das System $t = T'$, $u = hU'$ eine Lösung der vorgelegten Glei-

chung $t^2 - Du^2 = m^2$ und man ist daher sicher, die Zahl hU' unter der Reihe der Zahlen u_0, u_1, u_2 ..... irgendwo anzutreffen; sei λ der Index, für welchen man $u_\lambda = hU'$ hat, so folgt $u_\lambda \equiv 0 \ (mod\ h)$ oder, da man $u_0 = 0$ hat, $u_\lambda \equiv u_0 \ (mod\ h)$. Also wird der dritten Congruenz Genüge geleistet durch die Annahme $k = \lambda$. Zugleich sieht man ein, dass keine der Zahlen u, welche einen kleineren Index als λ hat, der nämlichen Congruenz Genüge leisten kann; denn wäre $l < \lambda$ und $u_l = hv'$, so wäre v' nothwendig kleiner als U', weil die Zahlen u mit wachsenden Indices zunehmen, und man hätte, da das System $t = t_l$ und $u = u_l$ die gegebene Gleichung auflösen müsste, die Gleichung $t_l^2 - Dh^2v^2 = m^2$, d. h. es gäbe eine kleinere Zahl $u' = v'$, als die kleinste $u' = U'$, welche die Gleichung $t'^2 - h^2Du'^2 = m^2$ befriedigt.

Wenn nun, indem man $k = \lambda$ setzt, mit dieser Congruenz $u_k \equiv u_0$ $(mod\ h)$ zugleich die drei anderen behaupteten Congruenzen statt hätten, so wäre der Satz bewiesen; er wird aber auch noch bewiesen sein, wenn, sobald diese drei Congruenzen für $k = \lambda$ entweder alle oder doch zum Theil nicht gültig sind, von uns bewiesen wird, dass alle die vier behaupteten Congruenzen gleichzeitig unter der Annahme $k = 2\lambda$ bestehen.

Vermöge der Werthe von t_e und u_e kann man ohne Mühe die Relation $(t_\lambda)^2 + D(u_\lambda)^2 = \frac{m^2}{2}\left(\frac{T}{m} + \frac{U\sqrt{D}}{m}\right)^{2\lambda} + \frac{m^2}{2}\left(\frac{T}{m} - \frac{U\sqrt{D}}{m}\right)^{2\lambda}$ verificiren, welche, wie man sogleich sieht, identisch dieselbe ist, wie $(t_\lambda)^2 - D(u_\lambda)^2 = mt_{2\lambda}$; hieraus folgt $t_{2\lambda} = \frac{1}{m}\left((t_\lambda)^2 + D(u_\lambda)^2\right) = \frac{1}{m}(m^2 + 2D(u_\lambda)^2) = m + \frac{2D(u_\lambda)^2}{m}$, also, da man $t_0 = m$ hat, $\frac{t_{2\lambda} - t^0}{h} = \frac{2D(u_\lambda)^2}{mh}$. Nun ist die Quantität $\frac{2D(u_\lambda)^2}{mh}$ eine ganze Zahl, weil zu Folge der Bestimmung von λ die Zahl h ein Theiler von u_λ und ferner m ein Theiler von $2D = 2b^2 + 2aa'$ ist. Also ist auch der Quotient $\frac{t_{2\lambda} - t_0}{h}$ eine ganze Zahl, d. h. es besteht unter der Annahme $k = 2\lambda$ die erste von den vier behaupteten Congruenzen, nämlich $t_k \equiv t_0 \ (mod\ h)$. — Man kann ferner ohne Schwierigkeit die Gleichung $u_{2\lambda} = \frac{2}{m} \cdot t_\lambda \cdot u_\lambda$ entweder sich verificiren oder in ähnlicher Weise, wie vorher die Gleichung $t_{2\lambda}$ sich herleiten. Nun ist $2t_\lambda$

theilbar durch m, weil $4(t_\lambda)^2 = 4D(u_\lambda)^2 + 4m^2$ durch m^2 theilbar ist, und u_λ theilbar durch h; also ist der Quotient $\frac{u_{2\lambda}}{h} = \left(\frac{2t_\lambda}{m}\right).\left(\frac{u_\lambda}{h}\right)$ eine ganze Zahl, oder es besteht, indem man wieder $k = 2\lambda$ setzt, die dritte der behaupteten Congruenzen, nämlich $u_k \equiv u_0 \pmod{h}$. — Weiter ist $t_{2\lambda+1} = T + \frac{2Du_\lambda u_{\lambda+1}}{m}$ und, da hier $2D = 2b^2 + 2aa'$ durch m und u_λ durch h theilbar ist, erhellt $t_{2\lambda+1} \equiv T \pmod{h}$ oder $t_{k+1} \equiv t_1 \pmod{h}$. — Endlich hat man $u_{2\lambda+1} = U + \frac{2t_{\lambda+1}u_\lambda}{m}$ und da die Zahl $2t_{\lambda+1}$ aus ähnlichen Gründen wie vorher die Zahl $2t_\lambda$ durch m theilbar ist und die Zahl u_λ durch h, so folgt $u_{2\lambda+1} \equiv U \pmod{h}$ oder $u_{k+1} \equiv u_1 \pmod{h}$. — Also existirt jedenfalls eine Zahl k, für welche unsere vier behaupteten Congruenzen gleichzeitig stattfinden.

Sechster Abschnitt.

Auflösung der allgemeinen Gleichung zweiten Grades zwischen den Unbestimmten X und Y.

§. 28.

Auflösung nach X und Y in ganzen Zahlen.

1) In der allgemeinen Gleichung zweiten Grades

$$(1)\quad aX^2+2bXY+cY^2+2dX+2eY+f=0$$

kann man, unbeschadet ihrer Allgemeinheit, immer die Zahlen a, b, c, d, e, f als ganz annehmen; denn sollte eine Gleichung gegeben sein, in der die Coefficienten von XY, X, Y entweder alle oder zum Theil ungerade Zahlen wären, so kann man sie durch Multiplication mit 2 auf die obige Form bringen. Um sie nun in ganzen Zahlen für X und Y aufzulösen, schliesse man vorläufig den Fall $b^2-ac=0$ aus, den wir einer besonderen Betrachtung vorbehalten, und transformire die vorgelegte Gleichung vermöge der (unter der Annahme einer von 0 verschiedenen Determinante $D=b^2-ac$ immer endlichen) Substitutionen:

$$(2)\quad X=\frac{x+cd-be}{b^2-ac},\ Y=\frac{y+au-bd}{b^2-ac};$$

die Gleichung (1) kommt dadurch zunächst auf die Form:

$$\begin{aligned} ax^2+2bxy+cy^2&+2x\left\{a(cd-be)+b(ae-bd)+d(b^2-ac)\right\}\\ &+2y\left\{b(cd-be)+c(ae-bd)+e(b^2-ac)\right\}\\ +\left\{a(cd-be)^2+2b(cd-be)(ae-bd)+c(ae-bd)^2\right\}&+2d(b^2-ac)(cd-be)\\ &+2e(b^2-ac)(ae-bd)+f(b^2-ac)^2=0,\end{aligned}$$

oder, wenn man bedenkt, dass die beiden Coefficienten von x und y verschwinden, und der von f unabhängige Theil des constanten Gliedes sich auf die Grösse $(b^2-ac)(ae^2-2bde+cd^2)$ reducirt, indem man der Kürze halber

$$(3)\quad M=(b^2-ac)(ae^2-2bde+cd^2)+f(b^2-ac)^2$$

setzt, einfacher:

$$(4)\quad ax^2+2bxy+cy^2=-M.$$

Diese letzte Gleichung enthält die Darstellung einer Zahl M durch die Form (a, b, c) und kann, wenn sie anders möglich ist, immer nach den Principien des vorigen Abschnittes in ganzen Zahlen für x und y aufgelöst werden. Indem man nun vermöge der Gleichungen (2) von den Werthen der x und y auf die Werthe der X, Y zurückgeht, wird nur in dem speciellen Falle $b^2-ac=1$ jedem ganzzahligen Systeme der x und y immer ein ganzzahliges System der X und Y entsprechen; in allen anderen Fällen kann es vorkommen, dass einige oder alle Werthe der X, Y sich als gebrochene Zahlen ergeben und mithin verworfen werden müssen. Hierbei sind nun folgende Fälle zu unterscheiden:

a) Die Gleichung (4) ist überhaupt in ganzen Zahlen für x und y nicht auflösbar: dieselbe Unmöglichkeit tritt dann auch für die Gleichung (1) ein.

b) Die Gleichung (4) hat eine negative Determinante oder eine positive quadratische Determinante mit der Nebenbedingung $M \gtrless 0$: sie hat alsdann eine begrenzte Menge von Auflösungen und die Gleichung (1) wird ebenfalls nur eine begrenzte Menge von Lösungen zulassen, nämlich so viele, als Systeme der x und y existiren, denen, wie der Versuch ausweist, ganzzahlige Werthe von X und Y entsprechen. Es kann hierbei der Fall vorkommen, dass kein System der x, y einem ganzzahligen Systeme der X, Y entspricht; die Zahl der Lösungen ist in diesem Falle 0.

c) Die Gleichung (4) hat eine positive nicht quadratische Determinante oder eine positive quadratische Determinante mit der Nebenbedingung $M=0$; die Anzahl der Lösungen nach x, y ist alsdann unbegrenzt (vorausgesetzt, dass

solche überhaupt möglich sind) und es existiren so viele Lösungen nach X, Y, als unter den unzählig vielen Systemen der x, y sich solche vorfinden, denen respective ganzzahlige Systeme der X und Y entsprechen.

Was die Fälle a) und b) anbetrifft, so ist dazu nichts weiter zu bemerken; dagegen was die Fälle unter c) anlangt, so tritt, da man bei der unendlichen Menge von Werthen der x und y ausser Stande ist mit jedem einzelnen Systeme den Versuch anzustellen, ob es eine Lösung nach X, Y giebt oder nicht, das Bedürfniss hervor nach einer Regel, vermöge derer diese Unterscheidung in durchgreifender Weise geleistet werden kann.

Betrachten wir zuerst den allgemeinen Fall einer positiven nicht quadratischen Determinante. Die Lösungen der Gleichung (4) haben alle die Form $x=\frac{1}{m}(Et+Fu)$, $y=\frac{1}{m}(Gt+Hu)$, wo t und u irgend welche Lösungen der Gleichung $t^2-Du^2=m^2$ bezeichnen. Indem wir daher unter t und u wesentlich positive Zahlenausdrücke verstehen, sind die Lösungen der Gleichung (4) nothwendig von einer der specielleren Formen:

$$(5)\quad\begin{cases} x=\frac{1}{m}(Et+Fu), & y=\frac{1}{m}(Gt+Hu);\\ x=\frac{1}{m}(Et-Fu), & y=\frac{1}{m}(Gt-Hu);\\ x=-\frac{1}{m}(Et-Fu), & y=-\frac{1}{m}(Gt-Hu);\\ x=-\frac{1}{m}(Et+Fu), & y=-\frac{1}{m}(Gt+Hu). \end{cases}$$

Jede dieser 4 Formen wird in jedem speciellen Falle besonders zu betrachten sein: aber da der Gang dieser Betrachtung für alle vier derselbe ist, wird es nur nöthig sein, denselben an einer zu zeigen, etwa an der ersten.

Substituiren wir also die erste der Formeln (5) in (2): wir erhalten dadurch:

$$(6)\quad X=\frac{Et+Fu+mcd-mbe}{m(b^2-ac)},\ Y=\frac{Gt+Hu+mae-mbd}{m(b^2-ac)};$$

und wollen nun die speciellen Werthe, welche X, Y annehmen, für irgend ein specielles Werthsystem $t=t_r$, $u=u_r$ bezeichnen mit X_r, Y_r. Was

nun die t, u anlangt, d. h. die Zahlenreihen $t_0, t_1, t_2, \ldots\ u_0, u_1, u_2, \ldots$, so wissen wir, einmal, dass sich dieselben vermöge der beiden linearen Recursionsformeln $t_{e+1}+t_{e-1}=\frac{2T}{m}t_e$ und $u_{e+1}+u_{e-1}=\frac{2T}{m}u_e$ formiren, und dann, dass, indem wir irgend eine beliebige Zahl h annehmen, immer eine unschwer zu bestimmende Zahl k existirt von der Beschaffenheit, dass die sämmtlichen Zahlen unserer beiden Reihen in k Gruppen untereinander nach dem Modul h congruente Zahlen zerfallen, deren jede eine unendliche Menge von Zahlenwerthen umfasst. Setzen wir also $h=m(b^2-ac)$ und bestimmen das zugehörige k; alsdann haben wir nur nöthig die k Systeme zusammengehöriger Werthe X_0 und Y_0, X_1 und Y_1, ... X_{k-1} und Y_{k-1} darauf hin zu untersuchen, ob sie ganzzahlig sind oder nicht; seien diejenigen darunter, welche ganzzahlig sind: X_α und Y_α, X_β und Y_β, X_γ und Y_γ, ..., so sind alle die unendlich vielen Systeme gleichfalls ganzzahlig, deren Indices e einer der Congruenzen

$$e \equiv \alpha,\ \beta,\ \gamma,\ \ldots\ (mod\ k)$$

Genüge leisten und alle solche Systeme, deren Indices keine dieser Congruenzen befriedigen, müssen verworfen werden; mit anderen Worten: alle Systeme, welche der nämlichen Gruppe zugehören, sind entweder zugleich ganzzahlig oder zugleich nicht ganzzahlig.

In der That, nehmen wir an, es bestehe z. B. die Congruenz $e\equiv\varepsilon$ $(mod\ k)$, so folgen die beiden Congruenzen $t_e\equiv t_\varepsilon$, $u_e\equiv u_\varepsilon$ $(mod\ 4)$ und hieraus durch Combination

$$Et_e+Fu_e+mcd-mbe \equiv Et_\varepsilon+Fu_\varepsilon+mcd-mbe\ (mod\ h);$$

sei nun der Rest, welchen die rechte Seite dieser Congruenz nach dem Divisor h lässt, gleich 0, so folgt, dass die linke Seite durch $h=m(b^2-ac)$ dividirt gleichfalls den Rest 0 lässt, d. h. wenn X_ε eine ganze Zahl ist, so ist auch X_e eine ganze Zahl; sei dagegen der Rest, welchen die rechte Seite der nämlichen Congruenz in Bezug auf den Divisor h lässt, von 0 verschieden, so entspricht derselbe Rest auch der linken Seite, d. h. wenn X_ε gebrochen ist, so ist auch X_e gebrochen. Ebenso beweist man, dass Y_ε und Y_e zu gleicher Zeit entweder ganz oder gebrochen sind und hierin liegt unser zu beweisender Satz.

Betrachten wir jetzt den speciellen Fall einer positiven quadratischen Determinante mit der Nebenbedingung $M=0$ (vergleiche hierüber §. 25.

2) am Schlusse). Wir wir wissen, existiren alsdann zwei von einander verschiedene Lösungssysteme der Gleichung (4), welche, indem f und g zwei relative Primzahlen und z eine beliebige ganze Zahl ausdrückt, beide die Form haben $x = fz$ und $y = gz$. Die Formeln (2) gehen dadurch über in:

$$(7)\quad X = \frac{fz + cd - be}{b^2 - ac},\quad Y = \frac{gz + ae - bd}{b^2 - ac}$$

und geben, wenn $b^2 - ac$ von 1 verschieden ist, im Allgemeinen gebrochene Werthe von X und Y. Um diejenigen Werthe von z zu bestimmen, für welche dies nicht eintritt, bemerken wir, dass, da die Zahlen f und g ausser 1 keinen gemeinschaftlichen Factor haben, die Gleichung $fm + gn = 1$ immer in ganzen Zahlen für m und n aufgelöst werden kann. Setzen wir in diese letzte Gleichung für f und g ihre Werthe aus (7), so geht dieselbe über in:

$$z = (b^2 - ac)(mX + nY) - m(cd - be) - n(ae - bd)$$

und substituiren wir diesen Werth von z wieder in die Gleichungen (7), so erhalten wir, wenn wir der Kürze halber $mX + nY = t$ setzen:

$$X = ft + \frac{(1 - fm)(cd - be) - fn(ae - bd)}{b^2 - ac},$$

$$Y = gt + \frac{(1 - gn)(ae - bd) - gm(cd - be)}{b^2 - ac},$$

oder, wenn wir für $1 - fm$ seinen Werth gn und für $1 - gn$ seinen Werth fm setzen:

$$(8)\quad X = ft + n.\frac{g(cd - be) - f(ae - bd)}{b^2 - ac},\quad Y = gt - m.\frac{g(cd - be) - f(ae - bd)}{b^2 - ac}.$$

Indem man in dieser Gleichung der Grösse t nach einander alle möglichen ganzzahligen Werthe ertheilt, bekommt man alle möglichen Werthe, deren X und Y fähig sind; dieselben werden alle entweder ganzzahlig ausfallen oder nicht, je nachdem die Grösse $g(cd - be) - f(ae - bd)$ ein genaues Multiplum von $b^2 - ac$ ist oder nicht ist. Also existiren im ersten Falle eine unbegrenzte Anzahl von Lösungen nach X, Y, im zweiten Falle existiren hingegen gar keine.

Beispiel 1. Die vorgelegte Gleichung sei:

$$2X^2 - 6XY + Y^2 - 14X + 10Y + 4 = 0,$$

also:

$$D = b^2 - ac = 7,\ cd - be = 8,\ ae - bd = -11,\ M = 581 = 7.83;$$

dann sind die Substitutionen, vermöge derer wir die Gleichung (4), nämlich

$$2x^2 - 6xy + y^2 = 581$$

erhalten, $X = \frac{x+8}{7}$, $Y = \frac{y-11}{7}$. Die Bedingungsgleichung ist $z^2 - 7 = 581s$ und wird aufgelöst vermöge Betrachtung der Congruenz $z^2 \equiv 7 \ (mod\ 581)$, welche sogleich in die beiden andern zerfällt $z^2 \equiv 7 \ (mod\ 7)$ und $z^2 \equiv 7 \ (mod\ 83)$. Die erste wird durch alle Werthe von z aufgelöst, welche Vielfache von 7 sind; die kleinste Lösung der zweiten ist $z = \pm 16$ und hieran knüpfen sich die beiden Lösungsreihen:

$+16, +99, +182, \ldots\ldots$ und $-16, +67, +150, +233, +316, +399, \ldots\ldots$

Aus den in denselben enthaltenen Zahlen haben wir diejenigen herauszusuchen, welche Vielfache von 7 sind und erhalten dadurch $z = 182$ und $z = 399$ als die einzigen positiven Lösungen, welche kleiner als 581 sind; die letzte hiervon ist aber auch identisch mit der Lösung $z = 399 - 581$ oder -182; unsere Bedingungsgleichung hat daher zwei Lösungen, die kleiner als der halbe Modul sind, und nicht mehr, nämlich:

$$z = +182, \ s = 57 \text{ und } z = -182, \ s = 57.$$

Betrachten wir zunächst die erste Lösung, so haben wir die beiden Formen $(2, -3, 1)$ und $(581, +182, 57)$ mit einander zu vergleichen. Das Resultat dieser Vergleichung ist die Formenreihe:

$(2, -3, 1)$, $(1, -4, 9)$, $(9, -14, 21)$, $(21, -28, 37)$, $(37, -46, 57)$, $(57, -182, 581)$, $(581, +182, 57)$,

vermöge deren man von der Form $2x^2 - 6xy + y^2$ zu der Form $581\xi^2 + 364\xi\eta + 57\eta^2$ übergehen kann. Der Uebergang geschieht, wie man leicht findet, durch die Transformation $x = -13\xi - 4\eta$, $y = -81\xi - 25\eta$ und zeigt, dass das System der Werthe $x = -13$, $y = -81$ eine Lösung der Gleichung $2x^2 - 6xy + y^2 = 581$ ist.

Um die übrigen Lösungen dieser Gleichung, welche der genannten liirt sind, zu finden, muss man die Gleichung $t^2 - 7u^2 = 1$ auflösen. Eine zu diesem Zwecke taugliche reducirte Form ist $(1, 2, -3)$ und man hat sich daher die Grösse $\frac{\sqrt{D} - b}{a} = \sqrt{7} - 2$ in einen Kettenbruch zu entwickeln. Man findet $\sqrt{7} - 2 = \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{4} + \frac{1}{1} + \ldots\ldots$

und hieraus in bekannter Weise die kleinste Lösung unserer Gleichung zwischen t und u, nämlich $T=8$, $U=3$. Hieraus leitet man vermöge der Recursionsformeln $t_{e+1}+t_{e-1}=16t_e$ und $u_{e+1}+u_{e-1}=16u_e$ nach und nach folgende Lösungssysteme her:

$$t_0=1,\ t_1=8,\ t_2=127,\ t_3=2024,\ t_4=32257,\ t_5=514088,$$
$$t_6=8193151,\ t_7=130576328,\ t_8=2081028097,\ \ldots\ldots$$
$$u_0=0,\ u_1=3,\ u_2=48,\ u_3=765,\ u_4=12192,\ u_5=194307,$$
$$u_6=3096720,\ u_7=49353213,\ u_8=786554688,\ \ldots\ldots$$

Man hat sich nun die Formeln zu entwickeln, vermöge derer man von diesen verschiedenen Zahlenwerthen der u und t aufsteigen kann zu den verschieden Zahlenwerthen der x, y: dieselben werden gefunden wie folgt:

$$x=-13t+42u,\ y=-81t+217u$$

und es ist hierzu nur noch die Bemerkung zu machen, dass diese Formeln gelten, wie beschaffen das Vorzeichen der t und u auch sein möge; mithin, wenn diese Grössen nur positiv genommen werden, zerfallen sie in die 4 bekannten Systeme von Formeln.

Wir müssen jetzt, ehe wir von x, y zu den X, Y übergehen, gemäss den eben entwickelten Regeln denjenigen speciellen Zahlenwerth k bestimmen, welcher dem hier in Anwendung kommenden Werthe von h, nämlich $h=m(b^2-ac)=7$, entspricht. Zu dem Zwecke muss man die kleinste Lösung der Gleichung $t'^2-h^2Du'^2=m$, d. h. hier die Gleichung $t'^2-343u'^2=1$ aufsuchen. Eine zur Auflösung dieser Gleichung taugliche Form ist (19, 1, —18) und dieselbe führt auf die Entwickelung von $\frac{\sqrt{D}-b}{a}=\frac{\sqrt{343}-18}{19}=\frac{7\sqrt{7}-18}{19}$ in einen Kettenbruch. Die Periode dieses Kettenbruches umfasst die Partialquotienten:

1 11 1 5 3 1 17 1 3 5 1 11 1 1 36 1

und führt auf folgende Zahlenwerthe, als die gesuchten kleinsten Lösungen nach t', u':

$$T'=130576328,\ U'=7050459;$$

hieraus ergiebt sich für die Gleichung $t^2-7u^2=1$ folgende Lösung als die entsprechende:

$$t=T'=130576328,\ u=7U'=49353213$$

und sehen wir zu, welches in den Reihen der Zahlen t_e, u_e der Index ist, für welchen dieselben mit den letztgenannten Zahlen zusammenfallen,

so finden wir $e = 7$. Also ist die Zahl k entweder 7 oder 14. Da aber die beiden Congruenzen $u_1 \equiv u_8$, $t_1 \equiv t_8$ $(mod\ 7)$ leicht constatirt werden können, so folgt $k = 7$.

Gehen wir jetzt zu den 4 verschiedenen Formelsystemen zurück, welche, unter der Annahme positiver t und u, die Werthe von x und y zulassen, nämlich:

$$\begin{aligned} x &= -13t+42u, & y &= -81t+217u, \\ x &= 13t+42u, & y &= 81t+217u, \\ x &= 13t-42u, & y &= 81t-217u, \\ x &= -13t-42u, & y &= -81t-217u \end{aligned}$$

und bemerken, dass wir dieselben nur für die Werthsysteme t_0 und u_0, t_1 und u_1, t_2 und u_2, t_3 und u_3, t_4 und u_4, t_5 und u_5, t_6 und u_6 zu untersuchen haben, sowie dass, wie aus der Betrachtung der Transformationsformeln

$$X = \frac{x+8}{7}, \quad Y = \frac{y-11}{7}$$

erhellt, die Zahlenwerthe von X und Y nur dann gleichzeitig ganz ausfallen können, wenn die entsprechenden Werthe von x den beiden Congruenzen

$$x \equiv -1, \; y \equiv -3 \; (mod\ 7)$$

Genüge leisten; alsdann ergeben sich der Reihe nach die folgenden Resultate:

I. Das erste System von Formeln liefert für keine t, u einen Werth von x, der congruent -1 wäre (sie sind vielmehr sämmtlich congruent $+1$): also fallen sämmtliche X gebrochen aus und ist das erste Formelsystem zu verwerfen. Aus vollkommen den nämlichen Gründen ist auch das vierte Formelsystem zu verwerfen.

II. Das zweite System von Formeln liefert für alle Werthe von t, u solche Werthe von x, die nach dem Modul 7 congruent mit -1 sind, und ebenso für alle Werthe von t, u solche Werthe von y, die congruent mit -3 sind. Demgemäss ist dasselbe für alle nur möglichen Werthe von t, u anwendbar. Ganz dasselbe gilt aus den nämlichen Gründen von dem dritten Formelsysteme. Setzen wir demgemäss die Werthe von x und y aus dem zweiten und dritten Formelsystem in die Ausdrücke für X, Y ein, so erhalten wir als zu dem Werthsysteme

$$Z = +182, \quad s = 57$$

gehörig folgende Lösungen der vorgelegten Gleichung:

$$X = \frac{13t+42u+8}{7}, \quad Y = \frac{81t+217u-11}{7};$$

$$X = \frac{13t-42u+8}{7}, \quad Y = \frac{81t-217u-11}{7}.$$

Das beiden Lösungssystemen gemeinschaftliche Paar zusammengehöriger Werthe von X und Y wird erhalten für $t=1$, $u=0$ und ist

$$X=3, \; Y=10.$$

Die den beiden Werthen $T=8$, $U=3$ entsprechenden kleinsten Lösungen sind respective:

$$X=34, \; Y=184 \text{ und } X=-2, \; Y=-2.$$

Es erhellt übrigens ganz von selbst, dass die ganze Rechnung, welche den Uebergang von den x, y zu den X, Y vermittelt, der grössten Abkürzungen fähig ist.

Zunächst hat man nicht nöthig die absoluten Werthe der t_e, u_e alle zu berechnen, sondern es genügen die kleinsten Reste nach dem Modul 7 und die Hülfsgleichung $t'^2 - 343u'^2 = 1$ ist vollständig überflüssig zur Berechnung des Werthes von k, die dem Modul $h=7$ entspricht: denn dieser Werth ergiebt sich ganz von selbst aus der Periodicität der Restwerthe von t_e und u_e. Die Rechnung ist in abgekürzter Weise wie folgt:

$$t_0 = 1, \; t_1 \equiv 1, \; t_2 \equiv 2.1-1 = 1, \; t_3 \equiv 2.1-1 = 1, \; t_4 \equiv 1, \; \ldots\ldots$$

$$u_0 = 0, \; u_1 = 3, \; u_2 \equiv 2.3-0 \equiv -1, \; u_3 \equiv 2.-1-3 \equiv +2,$$

$$u_4 \equiv 2.2+1 \equiv -2, \; u_5 \equiv 2.-2-2 \equiv +1, \; u_6 \equiv 2.1+2 \equiv -3,$$

$$u_7 \equiv 2.-3-1 \equiv 0, \; \ldots\ldots$$

also ist $k=7$. Die 4 Formelsysteme endlich, welche die verschiedenen Werthe von x, y geben, brauchen gleichfalls nur nach ihren kleinsten Resten in Betracht zu kommen und sie nehmen alsdann folgende Gestalt an:

$$x \equiv t, \; y \equiv 3t;$$

$$x \equiv -t, \; y \equiv -3t;$$

$$x \equiv -t, \; y \equiv -3t;$$

$$x \equiv t, \; y \equiv 3t.$$

Dadurch zieht sich die ganze oben durchgeführte Rechnung zu einer sol-

chen zusammen, die mit der grössten Leichtigkeit ausgeführt werden kann; denn setzt man hier überall für t den Restwerth 1 ein, so sieht man sofort ein, dass die beiden mittleren Systeme für alle Werthe von t, u zulässig sind, die beiden anderen dagegen für keine.

Wir haben noch zuzusehen, ob und wieviele Werthsysteme der X, Y existiren, welche der Lösung

$$z = -182, \quad s = 57$$

unserer Bedingungsgleichung, oder was dasselbe sagt, die der Form (581, —182, 57) liirt sind.

Lösen wir zuerst die Hülfsgleichung (4) auf. Der Uebergang von der Form (2, —3, 1) zu der Form (581, —182, 57) geschieht vermöge der Formenreihe:

(2, —3, 1), (1, 4, 9), (9, 14, 21), (21, 28, 37), (37, 46, 57), (57, 182, 581), (581, —182, 57)

und durch die folgende Nebenrechnung:

	1	2	2	2	4	0
$\frac{0}{1}$	$\frac{-1}{1}$	$\frac{-2}{1}$	$\frac{-3}{1}$	$\frac{-4}{1}$	$\frac{-13}{3}$	$\frac{+4}{-1}$

findet man die Transformationsformeln: $x = -13\xi + 4\eta$, $y = 3\xi - \eta$; also ist $x = -13$, $y = 3$ eine Lösung der Gleichung (4). Es ergeben sich hieraus die allgemeinen Formeln für x und y: $x = -13t - 42u$, $y = 3t - 35u$ oder, wenn wir für t und u nur positive Zahlenwerthe zulassen:

$$\begin{aligned} x &= -13t - 42u, & y &= 3t - 35u \\ x &= -13t + 42u, & y &= 3t + 35u \\ x &= 13t - 42u, & y &= -3t - 35u \\ x &= 13t + 42u, & y &= -3t + 35u \end{aligned}$$

und die Werthe von t und u sind wieder die sämmtlichen positiven Lösungssysteme der Gleichung $t^2 - 7u^2 = 1$, deren kleinste Reste nach dem Modul $h = m(b^2 - ac) = 7$ wir bereits berechnet haben. Die kleinsten Reste dieser 4 allgemeinen Lösungssysteme nach demselben Modul sind:

$$\text{I.} \begin{cases} x \equiv t, & y \equiv 3t, \\ x \equiv t, & y \equiv 3t, \end{cases}$$

$$\text{II.} \begin{cases} x \equiv -t, & y \equiv -3t, \\ x \equiv -t, & y \equiv -3t \end{cases}$$

und man folgert nun ganz in derselben Weise, wie vorhin, dass die auf die beiden Congruenzen I. bezüglichen Systeme der x, y zu verwerfen sind, dagegen die auf die beiden Congruenzen II. bezüglichen Systeme der x, y für alle Werthe von t, u den Uebergang zu brauchbaren Werthen von X, Y gestatten. Hiernach bekommen wir als zu dem Werthsysteme

$$s = -182,\ s = 57$$

gehörig folgende Lösungen der vorgelegten Gleichung:

$$X = \frac{13t - 42u + 8}{7},\ Y = \frac{-3t - 35u - 11}{7},$$

$$X = \frac{13t + 42u + 8}{7},\ Y = \frac{-3t + 35u - 11}{7}.$$

Beiden allgemeinen Systemen gemeinsam ist das specielle Paar zusammengehöriger X und Y:

$$X = +3,\ Y = -2$$

und den kleinsten Zahlen $T = 8$, $U = 3$ entsprechen respective folgende Paare zusammengehöriger Werthe:

$$X = -2,\ Y = -20 \text{ und } X = +34,\ Y = 10.$$

Beispiel 2. Die gegebene Gleichung sei

$$X^2 + 8XY + Y^2 + 2X - 4Y + 1 = 0$$

und geht zu Folge der Transformationsformeln

$$X = \frac{x+9}{15},\ Y = \frac{y-6}{15}$$

über in die einfachere Gleichung (4)

$$x^2 + 8xy + y^2 = -540\ (D = 15).$$

Die sämmtlichen Lösungen dieser Gleichung sind in folgenden 4 Systemen enthalten:

$$\begin{aligned} x &= 6t,\ y = -24t - 90u, \\ x &= 6t,\ y = -24t + 90u, \\ x &= -6t,\ y = 24t - 90u, \\ x &= -6t,\ y = 24t + 90u, \end{aligned}$$

wo t und u in unbestimmter Weise alle nur möglichen positiven Lösungen der Gleichung $t^2 - 15u^2 = 1$ bezeichnen. Die kleinste Lösung dieser Gleichung (wenn man von der Lösung $t = 1$, $u = 0$ absieht) ist $T = 4$, $U = 1$ und man findet mithin für die specielle Zahl $h = m(b^2 - ac) = 15$ als Modul folgende Restwerthe der aufeinanderfolgenden t_e, u_e (das zur

Berechnung dienende $\frac{27}{8}$ hat den Werth 8):

$$t_0 = 1,\ t_1 = 4,\ t_2 = 8\,.\,4 - 1 \equiv 1,\ t_3 \equiv 8\,.\,1 - 4 = 4,\ t_4 \equiv 1,\ t_5 \equiv 4, \ldots.$$

$$u_0 = 0,\ u_1 = 1,\ u_2 = 8 \equiv 8 - 7,\ u_3 \equiv 8\,.\,-7 - 1 \equiv +3,\ u_4 \equiv 8\,.\,3 + 7 \equiv 1,$$

$$u_5 \equiv 8\,.\,1 - 3 = 5,\ u_6 \equiv 8\,.\,5 - 1 \equiv -6,\ u_7 \equiv 8\,.\,-6 - 5 \equiv +2,$$

$$u_8 \equiv 8\,.\,2 + 6 \equiv 7,\ u_9 \equiv 8\,.\,7 - 2 \equiv -6,\ u_{10} \equiv -48 - 7 \equiv +5,$$

$$u_{11} \equiv 40 + 6 \equiv 1,\ u_{12} \equiv 8 - 5 = 3,\ u_{13} \equiv 24 - 1 \equiv -7,\ u_{14} = -56 - 3 \equiv 1,$$

$$u_{15} \equiv 8 + 7 \equiv 0, \ldots\ldots\ldots$$

also ist $k = 30$. Uebrigens, da die kleinsten Reste der Vielfachen von u, welche in den Ausdrücken für x und y vorkommen, gleich 0 sind, so war es nicht einmal unbedingt nöthig, die Restperiode der u sich zu beechnen und man hätte gleich unmittelbar zu dem nachfolgenden Raisonnement fortgehen können.

Die Transformationsformeln für X und Y zeigen, dass die Reste, welche x und y lassen müssen, damit X und Y ganze Zahlen werden, respective $+6$ und $+6$ sein müssen; nun erhellt entweder aus der directen Betrachtung der Formeln für x und y oder auch aus der Betrachtung ihrer kleinsten Reste nach dem Modul 15, dass dieser Umstand in den beiden ersten Formelsystemen eintritt für den Restwerth 1, welcher allen t mit geraden Indices zukommt, und nicht eintritt für den Restwerth 4, welcher allen t mit ungeraden Indices zukommt. Umgekehrt verhält es sich mit den beiden letzten Formelsystemen. Hiernach hat man folgende vier Lösungssysteme der vorgelegten Gleichung und sonst weiter keine:

$$X = \frac{6t_{2e} + 9}{15},\quad Y = \frac{-24t_{2e} - 90u_{2e} - 6}{15},$$

$$X = \frac{6t_{2e} + 9}{15},\quad Y = \frac{-24t_{2e} + 90u_{2e} - 6}{15},$$

$$X = \frac{-6t_{2e+1} + 9}{15},\quad Y = \frac{24t_{2e+1} - 90u_{2e+1} - 6}{15},$$

$$X = \frac{-6t_{2e+1} + 9}{15},\quad Y = \frac{24t_{2e+1} + 90u_{2e+1} - 6}{15}.$$

Die Grössen t_{2e}, t_{2e+1}, u_{2e}, u_{2e+1} haben hier die bekannte Bedeutung sämmtliche positive Lösungen der Gleichung $t^2 - 15u^2 = 1$ vorzustellen. Den beiden ersten Systemen gemeinsam zugehörig ist das Paar der Werthe von X und Y, welches für $t = 1$, $u = 0$ erhalten wird, nämlich

$$X = 1,\ Y = -2.$$

Die kleinsten Zahlen der beiden letzten Systeme werden für $e = 0$ erhalten, wodurch $t_{2e+1} = 4$, $u_{2e+1} = 1$ wird, nämlich

$$X = -1,\ Y = 0 \text{ und } X = -1,\ Y = 12.$$

2) In dem Vorhergehenden ist der Fall $b^2 - ac = 0$ ausdrücklich von der Erörterung ausgeschlossen worden und wir haben daher denselben nachträglich zu behandeln.

Sei μ der grösste gemeinschaftliche Theiler zwischen a und b und $\frac{a}{\mu} = \alpha$, $\frac{b}{\mu} = \beta$, so sind α und β relative Primzahlen unter einander und wenn man die Gleichung $b^2 - ac = 0$ durch μ^2 dividirt, geht sie über in $\beta^2 - \alpha . \frac{c}{\mu} = 0$, woher $c = \frac{\mu}{\alpha} . \beta^2$. Da nun α nicht in β aufgeht (ausser wenn $\alpha = 1$, in welchem Falle aber die nachfolgende Behauptung gleichwohl Geltung behält), so muss, damit die rechte Seite ganz ausfalle, nothwendig α in μ aufgehen und wir setzen daher $\frac{\mu}{\alpha} = m$. Dadurch wird

$$a = \alpha^2 m,\ b = \alpha\beta m,\ c = \beta^2 m$$

und die gegebene Gleichung lässt sich umschreiben, wie folgt:

$$m(\alpha X + \beta Y)^2 + 2dX + 2eY + f = 0.$$

Setzen wir jetzt $\alpha X + \beta Y = u$, so geht die vorhergehende Gleichung über in $2dX + 2eY + mu^2 + f = 0$ und man entwickelt sich jetzt aus dieser Gleichung und der Substitutionsgleichung für u leicht die folgenden Werthe von X und Y:

$$X = \frac{\beta mu^2 + 2eu + \beta f}{2(\alpha e - \beta d)},\ Y = -\frac{\alpha mu^2 + 2du + \alpha f}{2(\alpha e - \beta d)}.$$

Dieselben leisten, wie die Zahl u auch angenommen werden möge, der gegebenen Gleichung immer Genüge, sobald die Gleichung $\alpha e - \beta d$ von 0 verschieden ausfällt; mithin hat man nur noch nöthig diejenigen Werthe von u festzusetzen, für welche X und Y ganze Zahlen vorstellen.

Zunächst ist dazu nothwendig, wenn auch noch nicht hinreichend, dass u als eine ganze Zahl angenommen wird; dies geht unmittelbar aus der Betrachtung der Gleichung $z = \alpha X + \beta Y$ hervor. Setzen wir ferner den absoluten Werth des Nenners $2\alpha e - 2\beta d$ gleich h, so werden offenbar die Unbestimmten X, Y ganzzahlig werden für alle solche Zahlenwerthe von u, welche zu gleicher Zeit den beiden Congruenzen

$$\beta mu^2 + 2eu + \beta f \equiv 0,\ \alpha mu^2 + 2du + \alpha f \equiv 0 \pmod h$$

Genüge leisten. Wenn beide oder nur eine dieser Congruenzen unmöglich ist, so ist die vorgelegte Gleichung überhaupt nicht in ganzen Zahlen für X und Y aufzulösen; sind aber beide Congruenzen möglich, so suche man zunächst ihre sämmtlichen Lösungen in den kleinsten Zahlen zu bestimmen. Seien dieselben für die erste Congruenz

$$u \equiv \varepsilon', \varepsilon'', \varepsilon''', \ldots\ldots \varepsilon^{(n)} \pmod h$$

und für die zweite Congruenz

$$u \equiv \delta', \delta'', \delta''', \ldots\ldots \delta^{(\nu)} \pmod h):$$

so ist die vorgelegte Gleichung wiederum unmöglich, wenn unter den kleinsten Lösungen der ersten Reihe keine ist, die mit irgend einer kleinsten Lösung aus der zweiten Reihe übereinkäme; sind dagegen eine Anzahl von Lösungen für u beiden Reihen gemeinschaftlich, so existiren ebensoviele nach dem Modul h von einander verschiedene Systeme der u, für welche X, Y ganze Zahlen werden, und zwar enthält jedes System eine unendliche Menge von Zahlenwerthen der u, für welche dieses geleistet wird.

Wenn der Ausdruck $\alpha e - \beta d = 0$ ist, so findet die beschriebene Methode keine Anwendung mehr; es muss aber alsdann, da α und β relative Primzahlen zu einander sind, wegen der vorhergehenden Gleichung α in d und β in e aufgehen; wir setzen daher $\frac{d}{\alpha} = \frac{e}{\beta} = h$. Die gegebene Gleichung kann nun leicht auf die folgende Form gebracht werden:

$$m(\alpha X + \beta Y)^2 + 2h\alpha X + 2h\beta Y + f = 0$$

oder, wenn man mit m multiplicirt und zusammenzieht,

$$\left\{m(\alpha X + \beta Y) + h\right\}^2 = h^2 - mf.$$

Damit diese Gleichung möglich sei, ist nothwendig, dass $h^2 - mf$ ein vollständiges Quadrat sei. Dieses vorausgesetzt sei

$$h^2 - mf = k^2;$$

die vorige Gleichung zerfällt alsdann sofort in die beiden linearen Gleichungen:

$$m(\alpha X + \beta Y) + h + k = 0, \quad m(\alpha X + \beta Y) + h - k = 0$$

und diese beiden Gleichungen enthalten nothwendig alle Lösungen, deren die gegebene fähig ist.

Erinnern wir uns nun, dass α und β relative Primzahlen zu einander sind, so können folgende verschiedene Fälle eintreten. Die Zahl m ist

ein Theiler weder von $h+k$ noch von $h-k$: die gegebene Gleichung ist in ganzen Zahlen für X und Y unmöglich; die Zahl m ist ein Theiler nur von einer der Grössen $h+k$ und $h-k$: die gegebene Gleichung hat eine unendliche Menge von Lösungen, die aber alle nur ein einziges System congruenter Zahlen constituiren (sie gilt einer linearen Gleichung zwischen X, Y gleich); endlich die Zahl m ist ein Theiler sowohl von $h+k$, wie von $h-k$: die gegebene Gleichung hat wiederum eine unendliche Menge von Lösungen, die aber zwei Systeme congruenter Zahlen constituiren (sie gilt zwei linearen Gleichungen zwischen X und Y gleich).

Beispiel 1. Die vorgelegte Gleichung sei

$$3X^2 - 12XY - 12Y^2 + 2X + 4Y - 8 = 0,$$

also da man $3X^2 - 12XY + 12Y^2 = 3(X-2Y)^2$ hat, $m=3$, $\alpha=1$, $\beta=-2$, $ae-\beta d=4$, $f=-8$. Demgemäss wird

$$X = \frac{-6u^2+4u+16}{8},\ Y = -\frac{3u^2+2u-8}{8}$$

und die beiden aufzulösenden Congruenzen sind:

$$6u^2 - 4u - 16 \equiv 0,\ 3u^2 + 2u - 8 \equiv 0\ (mod\, 8).$$

Man kommt offenbar am kürzesten zum Ziele, wenn man alle nach dem Modul 8 verschiedene Werthe, also die Zahlen von 0 bis 7 durchprobirt. Man überzeugt sich leicht, dass beiden Congruenzen Genüge geschieh durch die Substitutionen von 0, 2, 4, 6 für u und es werden daher alle solche Werthe für u die Ausdrücke X und Y zu ganzen Zahlen machen, die einer der vier Congruenzen $u \equiv 0, 2, 4, 6\ (mod\ 8)$ Genüge leisten; mit andern Worten, die vorstehenden Formeln werden ganzzahlig, sobald man für u eine beliebige gerade Zahl einsetzt. Man bekommt hierdurch unter anderen folgende Systeme zusammengehöriger Werthe:

$X=2$, $Y=+1$; $X=0$, $Y=-1$; $X=-8$, $Y=-6$; $X=-22$, $Y=-14$.

Beispiel 2. Die vorgelegte Gleichung sei

$$4X^2 + 12XY + 9Y^2 + 8X + 12Y + 3 = 0;$$

alsdann ist $m=1$, $\alpha=2$, $\beta=3$, $\alpha e-\beta d = 2.6 - 3.4 = 0$; also hat man $\frac{d}{\alpha} = \frac{e}{\beta} = h = 2$ und man könnte nun die oben aufgestellten Formeln für die weitere Rechnung benutzen. Es ist indessen einfacher, dieselbe unmittelbar anzustellen und die gegebene Gleichung auf die Form $(2X+3Y)^2 + 4(2X+3Y) + 3 = 0$ zu bringen; weiter folgt $(2X+3Y+2)^2 = 1$, und die beiden linearen Gleichungen, in welche diese letztere zer-

fällt, sind $2X+3Y=-1$ und $2X+3Y=-3$. Mithin hat man die beiden Systeme

$$X=1\pm 3n,\quad Y=-1\mp 2n$$

und

$$X=\pm 3n,\quad Y=-1\mp 2n,$$

in denen für n der Reihe nach alle nur möglichen positiven Zahlen einzusetzen sind.

3) Auflösung der allgemeinen Gleichung zweiten Grades zwischen x und y in rationalen Zahlen.

Die vorhergegangenen Entwickelungen enthalten die ebensosehr durch die Tiefsinnigkeit ihrer Begründung, wie durch die Einfachheit der Endresultate ausgezeichnete Lösung des berühmten Problemes, die allgemeine Gleichung zweiten Grades zwischen x und y in ganzen Zahlen aufzulösen; sie zeigen aber zu gleicher Zeit auch, dass dies Problem in einer grossen Anzahl von Fällen unmöglich ist und es liegt darum der Gedanke nahe, das Problem von einem allgemeineren Gesichtspunkte aus aufzulösen, indem man die x und y blos der Bedingung unterwirft, rationale Zahlen darzustellen. Wir werden die Auflösungsmethode von Lagrange darstellen, welchem nach Gauss die Zahlentheorie in der neueren Zeit wohl das Meiste verdankt.

Sei die vorgelegte Gleichung zweiten Grades

$$ax^2+bxy+cy^2+dx+ey+f=0,$$

in welcher die Coefficienten a, b, c, d, e, f alle ganzzahlig sind. Die algebraische Auflösung dieser Gleichung nach vorhergegangener Multiplication mit $4a$ liefert uns

$$\begin{aligned}(2ax+by+d)^2 &= (d+by)^2-4a(f+ey+cy^2)\\ &= (b^2-4ac)y^2+2(bd-2ae)y+d^2-4af.\end{aligned}$$

Setzen wir hier der grösseren Kürze halber

$$2ax+by+d=t,\quad b^2-4ac=A,\quad bd-2ae=g,\quad d^2-4af=h,$$

so lässt sich die gegebene Gleichung ersetzen durch das System der beiden neuen Gleichungen:

$$2ax+by+d=t,\quad Ay^2+2gy+h=t^2.$$

Multipliciren wir die letzte mit A und setzen

$$Ay+g=u,\quad g^2-Ah=B,$$

so geht sie über in

$$u^2-At^2=B.$$

Auf diese Weise haben wir unsere ursprüngliche Gleichung zwischen x, y in eine einfachere zwischen t, u transformirt und wir können immer sämmtliche Lösungen der ersten erhalten, wenn wir die sämmtlichen Lösungen der zweiten haben. In der That, es ergeben sich ohne Schwierigkeit die Formeln

$$y = \frac{u - g}{A}, \quad x = \frac{t - by - d}{2a},$$

vermöge deren man von den Werthen der t, u zurückgehen kann auf die Werthe der y, x, und da dieselben in Bezug auf die vier Unbestimmten x, y, t, u lineär sind, so erhellt sofort, dass jeder rationalen Lösung nach t, u eine und nur eine rationale Lösung nach x, y entspricht und umgekehrt, dass jeder rationalen Lösung nach x, y eine und nur eine rationale Lösung nach t, u entspricht. Mithin giebt es ebensoviele Lösungen nach t, u, wie nach x, y und die letzteren können sämmtlich aus den ersteren gezogen werden.

Also sind wir berechtigt, an Stelle der vorgelegten Gleichung die transformirte Gleichung

$$u^2 - At^2 = B$$

zu discutiren. Nun ist klar, welches auch die Zahlenwerthe von u und t sein mögen, so kann man sie sich immer auf gleiche Benennung gebracht denken und demnach, indem z ihren kleinsten gemeinschaftlichen Nenner und daher x, y, z ganze Zahlen bezeichnen, die keinen die Einheit übersteigenden gemeinschaftlichen Theiler besitzen, $u = \frac{x}{z}$, $t = \frac{y}{z}$ setzen. Dadurch bekommen wir als identisch dasselbe wie die vorige ausdrückend die neue Gleichung

$$\text{I.} \quad x^2 - Ay^2 = Bz^2.$$

Wir dürfen überdies in dieser Gleichung von den Coefficienten A, B annehmen, dass keiner von ihnen einen quadratischen Factor grösser als 1 enthält; denn sollte dieses der Fall sein, so kann man sie immer durch einfache lineäre Substitutionen in eine Gleichung von derselben Form $x'^2 - A'y'^2 = B'z'^2$ transformiren, in der A' und B' keine quadratische Theiler enthalten. Sei nämlich $A = A'k^2$, $B = B'l^2$, so wird dieses geleistet durch die Substitutionen $x = x'$, $y = \frac{1}{k}y'$, $z = \frac{1}{l}z'$.

Indem wir also annehmen, dass in unserer Gleichung I x, y, z keinen gemeinschaftlichen Theiler > 1 besitzen und A und B ohne qua-

dratische Factoren sind, folgt noch, dass auch nicht einmal irgend welche zwei der Unbestimmten einen gemeinschaftlichen Divisor > 1 haben. Denn wäre ein solcher z. B. zwischen x und y vorhanden und gleich ϑ, so wäre ϑ^2 ein Theiler von x^2 und y^2 und mithin auch von Bz^2. Das geht aber nicht an, da ϑ^2 weder ein Theiler von z^2 noch von B sein darf und sich auch nicht auf beide Factoren vertheilen kann; denn dann würde immer noch auf B ein quadratischer Factor kommen. Ebenso beweist man, dass x und z relative Primzahlen sind, sowie y und z. Wir können ferner behaupten, dass A und B unbeschadet der Allgemeinheit als positive Grössen angenommen werden können. Zunächst sieht man, dass die Annahme: A und B beide negativ, nicht statthaft ist, weil dann die Summe zweier positiver Grössen negativ ausfiele. Mithin bleiben, wenn man die verschiedenen Vorzeichencombinationen berücksichtigt, nur drei verschiedene Fälle möglich, nämlich $x^2 - Ay^2 = +Bz^2$, $x^2 - Ay^2 = -Bz^2$, $x^2 + Ay^2 = +Bz^2$. Von diesen fallen aber der zweite und dritte zusammen, wie aus einer einfachen Vertauschung der Buchstaben A und B, sowie der Veränderlichen y und z erhellt und im dritten Falle erhält man durch Multiplication mit B die Gleichung $Bx^2 + ABy^2 = B^2z^2$, welche durch die lineäre Transformation $Bz = x'$, $x = z'$, $AB = A'$ übergeht in $x'^2 - A'y^2 = Bz'^2$. Endlich können wir noch $A \geqq B$ annehmen; denn wäre $A < B$, so würden wir blos die Gleichung durch Transposition ihrer Glieder auf die Form $x^2 - Bz^2 = Ay^2$ zu bringen haben.

Fassen wir alle die verschiedenen Eigenschaften zusammen, welche wir der Gleichung I. beilegen dürfen, so sind es folgende: 1) Je zwei der Veränderlichen sind relative Primzahlen zu einander; 2) jeder der beiden Coefficienten A und B ist ohne quadratischen Theiler; 3) die beiden Coefficienten A und B sind positiv und $A \geqq B$.

Dieses alles vorausgesetzt existiren, wenn die gegebene Gleichung möglich ist, d. h. wenn für x, y und z ganze Zahlen existiren, die die Gleichung I. befriedigen, immer solche ganzzahlige Werthe für n und z', welche der Gleichung

$$x = nz - z'A$$

Genüge leisten; denn z und A sind nothwendig relative Primzahlen, weil, wenn sie einen gemeinschaftlichen Theiler hätten, derselbe wegen der Gleichung I. auch ein Theiler von x sein müsste, also x und z keine

relativen Primzahlen zu einander sein könnten. Setzen wir diesen Ausdruck für x in unsere Gleichung I. ein, so erhält man nach einigen einfachen Umformungen:

$$\frac{n^2-B}{A}z^2-2nzz'+Az'^2=y^2$$

und da n, z, z', y lauter ganze Zahlen und ausserdem A gegen z eine relative Primzahl ist, folgt $\frac{n^2-B}{A}=num.\,integ.$, oder die Congruenz

$$n^2\equiv B\ (mod\ A)$$

ist immer möglich, sobald die gegebene Gleichung I. als möglich vorausgesetzt wird, und umgekehrt, wenn diese Congruenz nicht möglich ist, d. h. wenn B ein quadratischer Nichtrest von A ist, so ist auch die Gleichung I. unmöglich.

Gehen wir jetzt von dieser Congruenz aus, deren Verknüpfung mit der Möglichkeit der vorgelegten Gleichung wir soeben dargethan haben, und nehmen an, die Zahl n stelle speciell irgend eine beliebige ihrer kleinsten Lösungen dar, so ist der Bruch $\frac{n^2-B}{A}$ nothwendig positiv und kleiner als $\frac{A}{4}$. Setzen wir, um dieses zu zeigen, seinen Werth gleich s, so ist $n^2-B=As$ oder $n^2+(A-B)=A(s+1)$, wo $A-B$ zufolge der Voraussetzung eine wesentlich positive Grösse ist, wenigstens, wenn A nicht $=B$ ist, ein Fall, den wir nachher besonders betrachten werden. Nun ist n als eine kleinste Lösung der obigen Congruenz kleiner als der halbe Modul, also $n^2\leqq\frac{1}{4}A^2$. Setzen wir dies in die vorige Gleichung ein, so geht sie über in die Ungleichung $\frac{1}{4}A^2+A-B\geqq A(s+1)$, also ist auf jeden Fall noch stärker $\frac{1}{4}A^2+A>A(s+1)$; hieraus zieht man $s<\frac{1}{4}A$. — Dass die Grösse s wesentlich positiv ist, erhellt aus der Gleichung $n^2+A-B=A(s+1)$, deren linke Seite als die Summe zweier positiven Grössen gleichfalls positiv sein muss.

Nehmen wir an, der grösste quadratische Factor, welchen das derartig bestimmte s enthält, sei k^2, so kann man $s=A'k^2$ setzen und A' wird ebenso wie s der Ungleichung $A'<\frac{A}{4}$ Genüge leisten. Hierauf setzen wir in die obige Gleichung $\frac{n^2-B}{A}z^2-2nzz'+Az'^2=y^2$ für $\frac{n^2-B}{A}$ seinen Werth $A'k^2$ ein, und erhalten $A'k^2z^2-2nzz'+Az'^2=y^2$. Dieser Gleichung geben wir nach vorhergegangener Multiplication mit $A'k^2$ die

Form $(A'k^2z - nz')^2 - (n^2 - AA'k^2)z'^2 = A'k^2y^2$ und setzen $A'k^2z - nz' = x'$ und $ky = y'$. Berücksichtigen wir noch, dass zu Folge der Gleichung $\frac{n^2 - B}{A} = A'k^2$ der Ausdruck $n^2 - AA'k^2$ dem Coefficienten B gleich wird, so bekommen wir dadurch die transformirte Gleichung $x'^2 - Bz'^2 = A'y'^2$ oder

$$x'^2 - A'y'^2 = Bz'^2,$$

welche von derselben Form wie I. ist und in der nur der Coefficient A in den kleineren, aber immer noch positiven Coefficienten A' umgewandelt erscheint. Zugleich erhellt, dass diese transformirte Gleichung möglich ist, sobald es die ursprüngliche ist; denn der Uebergang zwischen beiden wird vermittelt durch die linearen Gleichungen

$$x = nz - Az', \; A'k^2z - nz' = x', \; ky = y'.$$

Vergleichen wir die beiden Coefficienten A' und B der transformirten Gleichung, so kann es immer noch vorkommen, dass $A' > B$ geblieben ist. In diesem Falle mache man sie zu dem Ausgangspunkte einer neuen Transformation, vermöge deren die zweite transformirte Gleichung

$$x''^2 - A''y''^2 = Bz''^2$$

mit dem noch weiter verkleinerten Coefficienten A'' erhalten wird. Derselbe wird dadurch bestimmt, dass man die kleinste Lösung der Congruenz $n'^2 \equiv B \; (mod\; A')$ sich bestimmt und darauf aus dem Werthe des Quotienten $\frac{n'^2 - B}{A'}$ alle quadratischen Factoren wegwirft. Diese Congruenz ist immer möglich; denn aus der vorhergehenden Gleichung $\frac{n^2 - B}{A} = A'k^2$ ergiebt sich $n' = n$ als eine specielle Lösung und die allgemeine ist daher $n' = mA'$: man hat sich mithin n' als die kleinste Lösung der Congruenz $n' \equiv n \; (mod\; A')$ zu bestimmen, und hierauf den Ausdruck $\frac{n'^2 - B}{A'} = A''k'^2$ zu formiren.

Ist auch jetzt noch $A'' > B$, so hat man die Transformation noch weiter und so lange fortzusetzen, bis man schliesslich auf einen Coefficienten $C = A^{(\nu)}$ kommt, der kleiner als B ist. Das Schema für diese Reihe von Transformationen ist folgendes:

$$\begin{array}{l|l} x^2 - Ay^2 = Bz^2 & \\ x'^2 - A'y'^2 = Bz'^2 & n^2 - B = AA'k^2, \quad n \leqq \tfrac{1}{2}A \\ x''^2 - A''y''^2 = Bz''^2 & n'^2 - B = A'A''k'^2, \quad n' \leqq \tfrac{1}{2}A', \quad n' \equiv n \pmod{A'} \\ x'''^2 - A'''y'''^2 = Bz'''^2 & n''^2 - B = A''A'''k''^2, \quad n'' \leqq \tfrac{1}{2}A'', \quad n'' \equiv n' \pmod{A''} \\ & \cdots\cdots\cdots\cdots \\ & \cdots\cdots\cdots\cdots \\ x^{(\nu)2} - A^{(\nu)}y^{(\nu)2} = Bz^{(\nu)2} & n^{(\nu-1)2} - B = A^{(\nu-1)}A^{(\nu)}k^{(\nu-1)2}, \quad n^{(\nu-1)} \leqq \tfrac{1}{2}A^{(\nu-1)}, \\ & \qquad n^{(\nu-1)} \equiv n^{(\nu-2)} \pmod{A^{\nu-1}} \end{array}$$

Die zuletzt erhaltene Form $x^{(\nu)2} - A^{(\nu)}y^{(\nu)2} = Bz^{(\nu)2}$ wird man nun umschreiben wie folgt: $x^{(\nu)2} - Bz^{(\nu)2} = Cy^{(\nu)2}$ und zum Ausgangspunkte neuer Transformationen machen, die zum Zwecke haben den Coefficienten B zu verkleinern, der jetzt dieselbe Rolle gegen C spielt, wie vorher A gegen B. Auf diese Weise wird man zuletzt eine transformirte Gleichung $x^{(\mu)2} - Dz^{(\mu)2} = Cy^{(\mu)2}$ erhalten, in der D kleiner als C ist und wird dann, indem wir die Gleichung umgekehrt schreiben, nämlich $x^{(\mu)2} - Cy^{(\mu)2} = Dz^{(\mu)2}$, dasselbe Spiel der Verkleinerung mit C fortsetzen, bis man endlich durch diese fortwährende Verkleinerung irgend einen Coefficienten gleich 1 erhält. Dies muss nothwendig irgend einmal eintreten; denn da diese Coefficienten immer ganz bleiben, so können sie sich nicht bis ins Unendliche verkleinern und man erhält also schliesslich eine Gleichung von der Form

$$\xi^2 - \eta^2 = M\zeta^2.$$

Zugleich, da alle die angewandten Transformationen lineär sind, so wird sich aus denselben eine gleichfalls lineäre Transformation x, y, z in die ξ, η, ζ zusammensetzen lassen und man wird daher die sämmtlichen Lösungen nach x, y, z aus den Lösungen der letzten reducirten Gleichung ziehen können. Nun kann aber diese immer in endlicher Weise gelöst werden; denn wenn man sich M in zwei Factoren α und β zerlegt, was, unter der Annahme, dass diese Factoren auch der Einheit gleich genommen werden dürfen, immer möglich ist, so geschieht der Gleichung offenbar Genüge, indem man setzt $\zeta = pq$, $\xi + \eta = \alpha p^2$, $\xi - \eta = \beta q^2$ und hieraus ergiebt sich, indem p und q vollkommen willkürliche Zahlen bezeichnen, das Lösungssystem

$$\zeta = pq, \ \eta = \frac{\alpha p^2 - \beta q^2}{2}, \ \xi = \frac{\alpha p^2 + \beta q^2}{2}.$$

Es ist bisher von einem Falle abgesehen worden, der eintreten kann, nämlich dass entweder in der gegebenen Gleichung oder auch im Verlaufe

der Transformation die beiden Coefficienten A und B einander gleich werden können. Es ist dann allemal eine Gleichung von der Form

$$x^2 - Ay^2 = Az^2$$

aufzulösen. Gemäss der auseinandergesetzten Methode hat man Behufs Bildung der transformirten Gleichung in den Ausdruck $n^2 - B = AA'k^2$ für n den Werth 0 einzusetzen und erhält dadurch, da man $B = A$ hat, $-1 = A'k^2$, also $A' = -1$, im Widerspruche dazu, dass sonst A' immer positiv ausfällt. Aber man kann diesen Uebelstand leicht vermeiden, wenn man für n nicht den Werth 0, sondern den Werth a einsetzt, wodurch $A^2 - A = AA'k^2$, also $A - 1 = A'k^2$ wird. Die weitere Rechnung geht in derselben Weise fort; denn offenbar ist A' eine positive Grösse und, wenn nicht kleiner als $\frac{A}{4}$, doch wenigstens kleiner als A, sodass factisch wenigstens die Verkleinerung fortgeht. Die Methode hat also die erforderliche Allgemeinheit.

Uebrigens ist auch eine besondere, der Natur dieses speciellen Falles angepasste Methode anwendbar. Da nämlich A in x aufgehen muss, so kann man $x = Au$ setzen und erhält dadurch $y^2 + z^2 = Au^2$. In dieser Gleichung sind z und A relative Primzahlen, weil es sonst y und z nicht sein könnten, und man kann also, immer die Möglichkeit der vorgegebenen Gleichung vorausgesetzt, die Zahlen n und y' sich so bestimmt denken, dass sie der Gleichung $y = nz + Ay'$ genügen. Indem man diesen Werth von y einsetzt, verwandelt sich die primitive Gleichung in die folgende: $\frac{n^2+1}{A} z^2 + 2nzy' + Ay'^2 = u^2$ und es muss hier $\frac{n^2+1}{A}$ eine ganze Zahl sein. Man kann also, indem k^2 den grössten gemeinschaftlichen Theiler dieser ganzen Zahl bezeichnet, $\frac{n^2+1}{A} = A'k^2$ setzen und hat dann $A'k^2z^2 + 2nzy' + Ay'^2 = u^2$, woher $(A'k^2z + ny')^2 - (n^2 - AA'k^2)y'^2 = A'k^2u^2$, oder, wenn man $A'k^2z + ny' = z'$, $ku = u'$ setzt und berücksichtigt, dass man $n^2 - AA'k^2 = -1$ hat,

$$z'^2 + y'^2 = A'u'^2.$$

Mithin ist die gegebene Gleichung zurückgeführt auf eine ähnliche, in welcher der Coefficient $A' < \frac{1}{4}A + \frac{1}{A}$ ist (in der Voraussetzung wenigstens, dass n die kleinste Lösung der Congruenz $n^2 + 1 \equiv 0 \pmod{A}$ bezeichnet). Indem man diese Gleichung einer neuen Transformation un-

terwirft und so fortfährt, wird man, da die Coefficienten A, A', A'', ... immer kleiner werden, schliesslich auf eine Gleichung von der Form $\zeta^2+\eta^2=v^2$ kommen, welche unter der Annahme $M=1$ nicht wesentlich verschieden ist von der Gleichung $\xi^2-\eta^2=M\zeta^2$ und daher gleich dieser aufgelöst werden kann. Von den Lösungen dieser letzten Gleichung aber kann man allmählig zu den Lösungen der ursprünglichen Gleichung aufsteigen.

Es ergiebt sich übrigens, ähnlich wie im allgemeinen Falle für diejenigen Transformationen, die den Coefficienten B unverändert lassen und nur den Coefficienten verkleinern, dass alle Congruenzen, die man hierbei aufzulösen hat, eben weil sie nur A betreffen, alle vermittelst lineärer Congruenzen aus der ersten Congruenz $n^2 \equiv -1 \ (mod\ A)$ fliessen. Die Möglichkeit dieser letzten Congruenz ist also die nothwendige und zureichende Bedingung dafür, dass die Gleichung $z^2+y^2=Au^2$ in ganzen Zahlen für z, y, u bestehen könne; denn sobald diese Bedingung erfüllt ist, kann man immer von der gegebenen Gleichung zu der auflösbaren Gleichung $\zeta^2+\eta^2=v^2$ gelangen.

Beispiel. Die gegebene Gleichung sei $x^2-11y^2=5z^2$. Man findet als die erste transformirte Gleichung $\xi^2-y^2=5\zeta^2$ und die Auflösung dieser letzten Gleichung ist: $\xi=\frac{q^2+5p^2}{2}$, $y=\frac{5p^2-q^2}{2}$, $\zeta=pq$, mithin:

$$z=4pq+\frac{q^2+5p^2}{2},\ y=\frac{q^2-5p^2}{2},\ x=5pq+2q^2+10p^2.$$

Die auseinandergesetzte Lösungsmethode hat zu ihrer Voraussetzung die Möglichkeit der gegebenen Gleichung; indessen bei genauerer Betrachtung führt sie zu einem Theoreme, vermöge dessen wir hierüber a priori Aufschluss erhalten.

Das Wesen unserer Methode liegt doch darin, dass wir von der Gleichung $x^2-Ay^2=Bz^2$ durch eine Reihe lineärer Transformationen zu der Gleichung $\xi^2-\eta^2=M\zeta^2$ übergehen, deren Auflösung in unserer Gewalt steht. Zugleich haben wir gezeigt, dass, wenn die erstere möglich ist, dieser Uebergang sich immer bewerkstelligen lasse. Hieraus folgt die Möglichkeit oder Unmöglichkeit unserer Gleichung als identisch mit der Möglichkeit oder Unmöglichkeit des besagten Ueberganges. Prüfen wir näher, was dessen Ausführbarkeit bedingt. Zunächst sind dazu

erforderlich eine Reihe von Transformationen (die jedoch möglicher Weise sich auf eine einzige reduciren kann), welche B unverändert lassen und A verkleinern. Alle diese Transformationen, welche nach einander die Coefficienten A', A'', A''', ... $A^{(\nu)} = C$ liefern, sind an eine Reihe von Congruenzen geknüpft, von denen die erste nur dann möglich ist, wenn B ein quadratischer Rest von A ist, die übrigen aber, sobald die erste möglich ist, immer möglich sind (man vergleiche, um sich die Ueberzeugung zu verschaffen, obiges Schema). Wir folgern hieraus allgemein: *Die nothwendige und hinreichende Bedingung für die Möglichkeit einer Transformation, welche den grösseren Coefficienten unter den kleineren herabbringt* (oder wenigstens demselben gleich macht), *besteht darin, dass der kleinere Coefficient ein quadratischer Rest des grösseren Coefficienten sei.*

Nehmen wir demgemäss an, dass den Transformationen, welche die abwechselnde Verkleinerung der beiden Coefficienten bezwecken, die folgenden transformirten Gleichungen entsprechen:

$$x^2 - Ay^2 = Bz^2,\ x^2 - Bz^2 = Cy^2,\ x^2 - Cy^2 = Dz^2,$$
$$x^2 - Dz^2 = Ey^2,\ .....,$$

wo die Coefficienten A, B, C, D, E, ... den Ungleichungen $A > B > C > D > E$ ..... Genüge leisten, so sind die nothwendigen und hinreichenden Bedingungen für ihre Ausführbarkeit, dass die Zahlen B, C, D, E, ... quadratische Reste seien von A, B, C, D, ... Wenn umgekehrt diese Bedingungen alle erfüllt werden, so ist der Uebergang von der Gleichung $x^2 - Ay^2 = Bz^2$ zu der Gleichung $\xi^2 - \eta^2 = M\zeta^2$ möglich und damit die Möglichkeit der ersteren bewiesen.

Nun lässt sich zeigen, dass alle die genannten Bedingungen erfüllt werden, *wenn in der gegebenen Gleichung* $x^2 - Ay^2 = Bz^2$ *und ihrer ersten transformirten* $x^2 - A'y = Bz^2$ *jeder Coefficient den anderen zum quadratischen Reste hat.* Dies giebt drei verschiedene Bedingungen: 1) A ist ein Rest von B, 2) B ist ein Rest von A, 3) A' ist ein Rest von B. Zu diesen kommt scheinbar noch als 4te Bedingung die hinzu, dass B ein Rest von A' sei; aber ein Blick auf unser Schema zeigt, dass diese Bedingung immer erfüllt wird, sobald es die zweite wird.

Unsere Behauptung lässt auch die folgende bequemere Aussprache zu: Wenn in der primitiven Gleichung und ihrer ersten transformirten jeder Coefficient den anderen zum quadratischen Reste hat, so gilt das Nämliche von allen nachfolgenden transformirten Gleichungen.

Betrachten wir zunächst die transformirten Gleichungen, welche sich auf die Verkleinerung des Coefficienten A beziehen, nämlich: $x'^2 - A'y'^2 = Bz'^2$, $x''^2 - A''y''^2 = Bz''^2$, ... $x^{(\nu)2} - A^{(\nu)}y^{(\nu)2} = Bz^{(\nu)2}$, so haben wir bereits dargethan, dass dieselben alle möglich sind, wenn B ein quadratischer Rest von A ist, und da diese Voraussetzung zutrifft, liefert ein Einblick in unser Schema sogleich den Beweis, dass B ein quadratischer Rest von A', A'', A''', ... $A^{(\nu)}$ ist. Es sollen nun weiter auch umgekehrt A', A'', A''', ... $A^{(\nu)}$ quadratische Reste von B sein. Von A' gilt dies zu Folge der Voraussetzung; um den Beweis rücksichtlich der Zahl A'' zu führen, bemerken wir, dass A'' ein quadratischer Rest von B ist, wenn es ein quadratischer Rest jedes beliebigen Primfactors von B ist. Indem also ϑ irgend einen Primfactor von B bezeichnet, reicht es hin zu beweisen, dass A'' ein quadratischer Rest von ϑ sei. Dies erhellt unmittelbar, wenn A'' ein Vielfaches von ϑ ist; denn alsdann kommt A'' nach dem Modul ϑ mit 0 überein und 0 ist ein quadratischer Rest jeder beliebigen Zahl. Wenn dagegen A'' kein Multiplum von ϑ ist, also relative Primzahl zu ϑ, so beweisen wir dasselbe auf folgende Art.

Da A' ein quadratischer Rest von B ist, so ist es auch ein quadratischer Rest von ϑ; mithin ist die Congruenz $x^2 \equiv A' \pmod{\vartheta}$ in ganzen bestimmten Zahlen für x' möglich. Aus derselben folgt $A''x^2k'^2 \equiv A'A''k'^2 \pmod{\vartheta}$, also, wenn man für $A'A''k'^2$ seinen Werth $n'^2 - B$, oder vielmehr, weil $-B$ als ein Multiplum von ϑ weggeworfen werden kann, n'^2 setzt, $A''x'^2k'^2 \equiv n'^2 \pmod{\vartheta}$. Zu Folge dieser Congruenz muss $A''x'^2k'^2$ ein quadratischer Rest von ϑ sein und da dasselbe von den beiden Factoren x'^2 und k'^2 gilt, so muss auch, nach einem p. 227 unter c) aufgeführten Theoreme, wofern A'', sowie x' und k' von 0 verschieden sind, A'' ein quadratischer Rest von ϑ sein. Nun ist k' gemäss seiner Bestimmung nicht unter 1, also immer von 0 verschieden, und dazu, dass x' von 0 verschieden sei, ist die nothwendige und zureichende Bedingung, dass, wegen der Congruenz $x'^2 \equiv A' \pmod{\vartheta}$, A' kein Multiplum von

ϑ sei. Also wenn A' kein Multiplum von ϑ ist, haben wir bewiesen, dass A'' ein quadratischer Rest von ϑ sei. Dasselbe folgt aber, obgleich auf andere Art, auch wenn A' ein Multiplum von ϑ ist.

In diesem Falle kann man aus der Congruenz $n' \equiv n \pmod{A'}$ die einfachere ziehen: $n' \equiv n \pmod{\vartheta}$, woher $n'^2 - B \equiv n^2 - B \pmod{\vartheta^2}$, oder, wenn man für $n'^2 - B$ und $n^2 - B$ ihre Werthe setzt, $A'A''k'^2 \equiv AA'k^2 \pmod{\vartheta^2}$. Nun ist A' wohl durch ϑ theilbar, aber nicht durch ϑ^2 (weil es keine quadratischen Factoren enthalten darf); mithin kann die vorige Congruenz nur bestehen, wenn man $A''k'^2 \equiv Ak^2 \pmod{\vartheta}$ hat; also da Ak^2 ein quadratischer Rest von B und daher auch von ϑ ist, muss $A''k'^2$ gleichfalls ein quadratischer Rest von ϑ sein und dies setzt, da k' und A'' von 0 verschieden sind, voraus, dass A'' ein quadratischer Rest von ϑ sei.

Also auf jeden Fall, mag nun A' von 0 verschieden sein oder nicht, ergiebt sich A'' als Rest von B: aber es findet ein wesentlicher Unterschied im Beweise statt; der Beweis geht im ersten Falle blos darauf zurück, dass A' ein Rest von B und B ein Rest von A' sei; im zweiten Falle muss man aber noch weiter zurückgehen und A als einen Rest von B voraussetzen. Also analog, wenn A nach dem Modul ϑ von 0 verschieden ist, wird man daraus, dass A ein Rest von B und B ein Rest von A ist, den Schluss ziehen können, dass A' ein Rest von B sei, d. h. die dritte Bedingung aus den beiden ersten folge. Dagegen wenn A ein Multiplum von ϑ ist oder mit anderen Worten, da ϑ jeden Primfactor von B bezeichnen kann, keine relative Primzahl zu B ist, ist die dritte Bedingung keine nothwendige Folge der beiden ersten. Hieraus ergiebt sich also die wichtige Bemerkung, dass, wenn A und B relative Primzahlen zu einander sind, die dritte der aufgeführten Bedingungen eine einfache Folge der beiden ersten und daher überflüssig ist, dagegen, wenn A und B gemeinschaftliche Factoren besitzen, ist die dritte Bedingung nicht nothwendig eine Folge der beiden ersten und daher wesentlich.

Die Resultate der bisherigen Beweisführung können wie folgt zusammengefasst werden: Wenn 3 aufeinanderfolgende transformirte Gleichungen gegeben sind, die den gemeinschaftlichen Coefficienten B haben und deren nicht gemeinschaftliche Coefficienten respective durch die ab-

steigenden Zahlen A, A', A'' (übrigens alle drei $> B$) dargestellt werden, und wenn die Coefficienten der beiden ersten von einander respective quadratische Reste sind, so sind auch die Coefficienten A'' und B der letzten von einander respective quadratische Reste. Aus dieser Aussprache erhellt unmittelbar, wenn man von der zweiten und dritten transformirten auf die vierte und so fort schliesst, dass in allen transformirten Gleichungen, welche die Verkleinerung von A zum Zwecke haben, jeder Coefficient ein quadratischer Rest des anderen ist.

Den nämlichen Nachweis haben wir jetzt zu führen rücksichtlich des zweiten Systemes transformirter Gleichungen, welches sich auf die Verkleinerung von B bezieht und dessen Entstehung in folgendem Schema dargestellt werden kann:

$$x^2 - Bz^2 = Cy^2, \quad C = A^{(\nu)}$$

$$x'^2 - B'z'^2 = Cy'^2, \quad m^2 - C = BB'l^2, \quad m \leqq \tfrac{1}{2}B,$$

$$x''^2 - B''z''^2 = Cy''^2, \quad m'^2 - C = B'B''l^2, \quad m' \leqq \tfrac{1}{2}B, \quad m' \equiv m \pmod{B'},$$

. . . .

. . . .

Zu dem Zwecke haben wir jetzt offenbar nur nöthig zu zeigen, dass die beiden ersten Gleichungen des Systemes den in Rede stehenden Bedingungen Genüge leisten, d. h. dass B ein Rest von C und umgekehrt C ein Rest von B, sowie B' ein Rest von C und umgekehrt C ein Rest von B' sei. Die beiden ersten Aussagen folgen unmittelbar daraus, dass die erste Gleichung des zweiten Systemes identisch ist mit der letzten Gleichung des ersten Systemes; von den beiden letzten Aussagen ist die eine, dass C ein quadratischer Rest von B' sei, eine nothwendige Folge der Art und Weise, wie man sich m bestimmt hat, nämlich vermöge der Congruenz $m^2 \equiv C \pmod{B}$, d. h. mit anderen Worten, sie folgt daraus, dass C als ein Rest von B vorausgesetzt wird. Demgemäss bleibt nur noch die 4te Aussage, dass B' ein quadratischer Rest von C sei, zu beweisen übrig. Dieser Beweis ist wieder identisch mit dem Beweise, dass B' quadratischer Rest ist zu irgend einem beliebigen Primfactor ϑ von C.

Wenn B ein Multiplum von ϑ ist, so bedarf dies keines weiteren Beweises. Ist dagegen B' kein Multiplum von ϑ, so beweist man dasselbe auf folgende Art.

Da B ein quadratischer Rest von C ist, so ist B auch ein quadratischer Rest von ϑ, also die Congruenz $x^2 \equiv B \pmod{\vartheta}$ möglich. Hieraus folgt $B'x^2l^2 \equiv BB'l^2 \pmod{\vartheta}$, also wenn man für $BB'l^2$ seinen Werth $m^2 - C$ unter Vernachlässigung der Grösse $-C$ einsetzt, $B'x^2l^2 \equiv m^2 \pmod{\vartheta}$. Demgemäss ist, wie vorher, wenn B von 0 verschieden ist, B' ein quadratischer Rest von ϑ.

Es ist aber auch ein quadratischer Rest von ϑ, wenn B ein Multiplum dieser Grösse ist. Da $A^{(\nu-1)}$ ein Rest von B ist, so ist es alsdann auch ein Rest von ϑ und die Congruenz $x^2 \equiv A^{(\nu-1)} \pmod{\vartheta}$ möglich. Multipliciren wir dieselbe mit $A^{(\nu)}k^{(\nu-1)^2}$ und bemerken, dass auch $A^{(\nu)}$ den Factor ϑ enthält, so folgt $A^{(\nu)}k^{(\nu-1)}x^2 \equiv A^{(\nu-1)}A^{(\nu)}k^{(\nu-1)^2} \pmod{\vartheta^2}$ oder wenn wir, unter Benutzung des Schemas für unser erstes System, für die rechte Seite ihren Werth einsetzen und grösserer Einfachheit halber die Indices von k und n weglassen, sowie links für $A^{(\nu)}$ seinen Werth C einführen: $Ck^2x^2 \equiv n^2 - B \pmod{\vartheta^2}$. Nun ist die linke Seite, sowie das zweite Glied rechts in dieser Congruenz durch ϑ theilbar, also muss es auch das Glied n^2 sein und da ϑ eine Primzahl ist, folgt weiter, dass n^2 sogar durch ϑ^2 theilbar ist. Mithin kann man das Glied fortwerfen und erhält $Ck^2x^2 \equiv -B \pmod{\vartheta^2}$. Multiplicirt man jetzt mit $B'l^2$, so folgt $B'Ck^2l^2x^2 \equiv -BB'l^2 \pmod{\vartheta^2}$ oder, wenn man für $-BB'l^2$ seinen Werth setzt, $B'Ck^2l^2x^2 \equiv C - m^2 \pmod{\vartheta^2}$. Hier ist m^2 wieder aus ähnlichen Gründen, wie vorher n^2 durch ϑ^2 theilbar und kann daher gleichfalls wegfallen, so dass wir $B'Ck^2l^2x^2 \equiv C \pmod{\vartheta^2}$ erhalten. Diese Congruenz kann, da C durch ϑ, aber nicht durch ϑ^2 theilbar ist, nur bestehen, wenn man hat $B'k^2l^2x^2 \equiv 1 \pmod{\vartheta}$. Hiernach ist $B'k^2l^2x^2$ ein Rest von ϑ. Nun kann weder B', noch k, noch l, noch x gleich oder der 0 congruent sein. (Was namentlich x betrifft, so würde, wenn es gleich 0 wäre, zu Folge der Congruenz $x^2 \equiv A^{(\nu-1)} \pmod{\vartheta}$ auch $A^{(\nu-1)}$ der 0 congruent sein nach dem Modul ϑ, d. h. $A^{(\nu-1)}$ und $A^{(\nu)}$ hätten beide den Factor ϑ gemeinschaftlich und dies angewandt auf die Gleichung $n^2 - B = A^{(\nu-1)}A^{(\nu)}k^2$ würde zu Folge haben, B theilbar durch den quadratischen Factor ϑ^2). Also ist B' ein Rest von ϑ, wie zu beweisen.

Das zweite System unserer transformirten Gleichungen genügt demzufolge den oben bezeichneten Bedingungen und wir haben dies als eine

Folge davon erkannt, dass das erste eben diesen Bedingungen gleichfalls genügt. Analog genügt das dritte, weil das zweite genügt, und indem man endlich in der nämlichen Weise weiter fortschliesst, gelangt man zu der letzten Gleichung $\xi^2 - \eta^2 = M\zeta^2$, in der 1 ein Rest von M und M ein Rest von 1 ist. Hiermit haben wir den vollständigen Beweis geliefert, dass, wenn die obigen drei Bedingungen statthaben, in jeder transformirten Gleichung immer der eine Coefficient ein Rest des anderen Coefficienten ist, und können nun folgendes Theorem aussprechen:

Die nothwendige und zureichende Bedingung dafür, dass die Gleichung $x^2 - Ay^2 = Bz^2$ in ganzen Zahlen für x, y, z aufgelöst werden könne, ist, wenn A und B relative Primzahlen zu einander sind, dass A ein quadratischer Rest von B und B ein quadratischer Rest von A sei; wenn dagegen A und B keine relativen Primzahlen zu einander sind, so muss dieselbe Bedingung auch noch für die erste transformirte Gleichung erfüllt werden.

Das vorstehende Theorem lässt eine weit einfachere Aussprache zu. Nehmen wir an, der grösste gemeinschaftliche Theiler zwischen A und B sei a, so kann man $A = ab$, $B = ac$ setzen und weder a und c, noch a und b, noch auch b und c können einen gemeinschaftlichen Theiler > 1 haben. Substituiren wir ferner ax' für x, so kommt unsere Gleichung auf die Form

$$ax'^2 = by^2 + bz^2,$$

und damit dieselbe in ganzen Zahlen für x', y, z aufgelöst werden könne, sind die nothwendigen und hinreichenden Bedingungen: 1) ab muss ein Rest von ac und 2) umgekehrt ac ein Rest von ab sein und, indem man den verkleinerten Coefficienten ac in der ersten transformirten Gleichung mit A' bezeichnet, 3) A' muss ein Rest von ac sein. Dies giebt die drei Bedingungscongruenzen:

$$n^2 \equiv ac \ (mod\ ab),\ m^2 \equiv ab \ (mod\ ac),\ w^2 \equiv A' \ (mod\ ac).$$

Setzen wir, da n und m nothwendig durch a theilbar sind, $n = a\nu$, $m = a\mu$, so gehen die beiden ersten derselben über in

$$a\nu^2 \equiv c \ (mod\ b),\ a\mu^2 \equiv b \ (mod\ c),$$

deren Bestehen umgekehrt zur Folge hat, dass ac ein Rest von ab und ab ein Rest von ac ist. Es kommt nun darauf an die dritte Bedingungs-

congruenz in ähnlicher Weise umzugestalten. Den obigen Formeln gemäss ist $n^2 - B = AA'k^2$, oder, wenn man für n, B, A ihre Werthe av, ac, ab einführt, $a^2v^2 - ac = abA'k^2$, also ist $bA'k^2 \equiv -c \pmod{a}$ und, wenn man für A' den ihm nach dem Modul a congruenten Werth w^2 setzt, $b(wk)^2 \equiv -c \pmod{a}$. Umgekehrt, wenn die soeben erhaltene Bedingungscongruenz $bw^2 \equiv c \pmod{a}$ nach w möglich ist und gleichzeitig auch die beiden ersten transformirten Bedingungscongruenzen bestehen, so ist A' ein Rest von ac.

Um dieses zu beweisen, bemerken wir, dass, da die Congruenz $av^2 \equiv c \pmod{b}$ als möglich vorausgesetzt wird, die Zahlen v, A', k in bekannter Weise derartig bestimmt werden können, dass die Gleichung $a^2v^2 - ac = abA'k^2$ besteht. Aus derselben ergiebt sich einmal, dass k eine relative Primzahl zu a sein muss (denn die Annahme des Gegentheiles würde entweder darauf führen, dass einer der beiden Coefficienten a und c einen quadratischen Factor enthielte, oder dass sie beide einen gemeinsamen Theiler >1 besässen) und dann dass die Congruenz $bA'k^2 \equiv -c \pmod{a}$ erfüllt wird. Nun ist nach der Voraussetzung $bw^2 \equiv -c \pmod{a}$ möglich, also folgt $bw^2 \equiv bA'k^2$ oder, da b eine relative Primzahl zu dem Modul a ist, $w^2 \equiv A'k^2 \pmod{a}$, d. h. $A'k^2$ ist ein Rest von a. Hieraus folgert man ohne Schwierigkeit, da k^2 kein Vielfaches von a ist, dass auch A' ein Rest a sei.

Es bleibt jetzt nur noch zu zeigen übrig, dass A' auch ein Rest von c sei; denn alsdann ist es nothwendig ein Rest von ac. Zu dem Zwecke folgern wir aus der zuletzt genannten Gleichung die Congruenz $bA'k^2 \equiv av^2 \pmod{c}$ und schreiben hier für b den damit nach dem Modul c congruenten Werth $a\mu^2$: dadurch erhalten wir $aA'(\mu k)^2 \equiv av^2 \pmod{c}$, oder, da a eine relative Primzahl zu c ist, $A'(\mu k)^2 \equiv v^2 \pmod{c}$; also ist $A'(\mu k)^2$ ein Rest von c. Da nun auch $(\mu k)^2$ ein Rest von c ist und weder μ noch k einen Factor mit c gemeinschaftlich haben kann, so ergiebt sich hieraus, dass A' ein Rest von c sein muss.

Die Resultate unserer letzten Entwickelung lassen sich in folgendem Theoreme zusammenfassen: **Die nothwendigen und hinreichenden Bedingungen für die Möglichkeit der Gleichung $x^2 - Ay^2 = Bz^2$ sind, dass A ein Rest von B, sowie umgekehrt B ein Rest von A sei und ausserdem, indem a den grössten ge-**

meinschaftlichen Theiler von A und B bezeichnet, dass die Congruenz $Au^2 \equiv -B \pmod{a^2}$ bestehen könne; oder, noch anders ausgedrückt:

Die nothwendige und hinreichende Bedingung für die Möglichkeit der Gleichung

$$ax^2 = by^2 = cz^2,$$

in der die Zahlen a, b, c positiv und ohne alle quadratischen Factoren, sowie zu je zweien relative Primzahlen sind, ist die Möglichkeit der drei Congruenzen:

$$au^2 \equiv c \pmod{b},\ au^2 \equiv b \pmod{c},\ bu^2 \equiv -c \pmod{a}.$$

Die dritte Bedingung wird in dem Falle, in welchem A und B relative Primzahlen sind, d. h. wenn a gleich 1 ist, immer erfüllt und ist daher überflüssig, in Uebereinstimmung mit der weiter oben befindlichen Aussprache eben desselben Satzes.

